TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2013) 37: 571 – 576

doi:10.3906/mat-1202-30

Finite rings and Wilson's theorem

Yasuyuki HIRANO,[1,*] **Manabu MATSUOKA**[2]

[1]Naruto University of Education, 748 Nakashima Takashima Naruto Narutocity Tokushima 772-8502, Japan

[2]Kuwanakita-Highschool, 2527 Shimofukayabe Kuwana Mie 511-0808, Japan

Received: 11.02.2012 • **Accepted:** 06.06.2012 • **Published Online:** 12.06.2013 • **Printed:** 08.07.2013

Abstract: In this paper we consider the product of all elements in the group of units in a finite ring and we generalize Wilson's theorem to finite rings. As an application, we study some generalizations of Wilson's theorem on residually finite Dedekind domains. And we also give some examples for such rings. Moreover we study some generalizations of Wilson's theorem on rings of matrices over a finite commutative ring.

Key words: Finite rings, Wilson's theorem, residually finite Dedekind domains

1. Introduction

Wilson's theorem asserts that $(p-1)! \equiv -1 \pmod{p}$ for any prime p. C. F. Gauss generalized this theorem as follows: the product of the positive integers $< n$ and prime to n is congruent modulo n to -1 if $n = 4, p^k$ or $2p^k$, where p is an odd prime and k is a positive integer, but to $+1$ if n is not of one of these three forms (see [2, p. 65]).

Generalizations of Wilson's theorem have been extensively studied over several years (cf [1], [5], [8]). In this paper, we consider the product of all elements in the group of units in a finite ring and we generalize Wilson's theorem to finite rings.

We first restate Wilson's theorem and Gauss' generalization of Wilson's theorem in terms of rings and groups. In fact, these theorems mentioned the product of all invertible elements in some factor ring of the ring of integers. We classify finite commutative rings in which the product of all invertible elements is not 1 (Theorem 1). As an application, we apply this result to some special class of Dedekind domains and we also give some examples (Theorem 2). Finally we establish Wilson's theorem on rings of matrices over a finite ring (Theorem 3).

2. Some generalizations of Wilson's theorem

First we restate Wilson's theorem and Gauss' generalization of Wilson's theorem in terms of rings and groups. Those theorems are considered as results on some factor rings of the ring of integers. To state those, we introduce some notations. For a ring R, R^* denotes the group of units in R and $J(R)$ denotes the Jacobson radical

*Correspondence: yahirano@naruto-u.ac.jp

2010 *AMS Mathematics Subject Classification:* Primary 11T30; Secondary 11T06.

Dedicated to Professor Takao Sumiyama on his 60th birthday

of R. If G is a finite abelian group, then we denote the product of all elements in G by $G!$. Then Wilson's theorem and Gauss' generalization can be stated as follows:

Wilson's Theorem. *Let Z denote the ring of integers and p denote a prime number. Then $(Z/(p))^*! = -1$.*

Gauss' generalization of Wilson's Theorem (cf. [2, p.65]). *Let Z denote the ring of integers and n denote a positive integer. Then:*

$$(Z/(n))^*! = \begin{cases} -1 & \text{if } n = 4,\ p^k \text{ or } 2p^k \\ 1 & \text{otherwise,} \end{cases}$$

where p is an odd prime, and k is a positive integer.

We first generalize the latter theorem to finite rings. For fundamental results on finite rings, we refer the reader to McDonald [4].

Proposition 1 *Let G be a finite abelian group with identity e. If there is precisely one element a of order 2 in G, then $G! = a$. Otherwise, $G! = e$.*

Proof Set $H = \{x \in G \mid x^2 = e\}$. If $b \in G - H$, then $b^{-1} \neq b$. Hence there are elements $a_1, \ldots, a_n$ such that G is the disjoint union of $\{a_1, a_1^{-1}\}, \ldots, \{a_n, a_n^{-1}\}$ and H. Then we have $G! = a_1 a_1^{-1} \cdots a_n a_n^{-1} H! = H!$. If there is precisely one element a of order 2 in G, then $H = \{e, a\}$. In this case, we have $G! = H! = a$.

Next, suppose that there is no element of order 2 in G. Then there are elements $a_1, \ldots, a_n$ such that G is the disjoint union of $\{a_1, a_1^{-1}\}, \ldots, \{a_n, a_n^{-1}\}, \{e\}$. Then we have $G! = a_1 a_1^{-1} \cdots a_n a_n^{-1} e = e$.

Finally, suppose that the number of elements of order 2 in G is greater than one. By fundamental theorem of finite abelian groups, G is a finite direct sum of cyclic groups. Hence we can find two abelian subgroups G_1, G_2 of G such that $G = G_1 \times G_2$ and the orders of G_1 and G_2 are even. Then we can easily see that $G! = G_1!^{|G_2|} \cdot G_2!^{|G_1|} = e$. This completes the proof. □

Corollary 1 *Let $G = \{a_1, \ldots, a_n\}$ be a finite group with identity e. Let $D(G)$ denote the commutator subgroup of G. If there is precisely one element $aD(G)$ of order 2 in $G/D(G)$, then $a_1 \cdots a_n \in a^{|D(G)|}D(G)$. Otherwise, $a_1 \cdots a_n \in D(G)$.*

Lemma 1 *Let R be a finite commutative local ring with 1. If R^* is of odd order, then R is isomorphic to $GF(2^k)$ for some positive integer k.*

Proof Since $(-1)^2 = 1$ and since R^* is of odd order, we conclude $-1 = 1$, that is $2 = 0$. Since R is finite, $J(R)$ is nilpotent. If the Jacobson radical $J(R)$ of R is nonzero, then there is a nonzero element $a \in J(R)$ such that $a^2 = 0$. Then $1 + a(\neq 1)$ is an invertible element of order 2. This is a contradiction. Hence $J(R) = 0$, and so R is a finite field of characteristic 2. □

Theorem 1 *Let R be a finite commutative ring. Then $R^*! = 1$ except cases where R is a direct sum of finitely many (possibly zero) finite fields of characteristic 2 and one of the following rings:*

(A) *a finite commutative local ring of characteristic p^k, where p is an odd prime and k is a positive integer;*

(B) $Z/(4)$;

(C) $Z[x]/(4, 2x, x^2 - 2)$;

(D) $GF(2)[x]/(x^2)$;

(E) $GF(2)[x]/(x^3)$.

Proof By fundamental theorem of finite abelian groups, R^* is a finite direct product of cyclic groups. Assume that $R^* \neq \{1\}$. Hence there are invertible elements $a_1, \ldots, a_n \in R - \{1\}$ such that $R^* = < a_1 > \times \cdots \times < a_n >$. By Proposition 1, $R^*! \neq 1$ if and only if only one $< a_i >$ is of even order. Since R is a finite commutative ring, R is a direct sum of local rings.

So assume that $R^*! \neq 1$ and that $R = R_1 \oplus \cdots \oplus R_m$, where each R_i is a local ring. Then only one of the R_i's, say R_1, is of even order. By Lemma 1, all $R_2, \ldots, R_m$ are finite fields of characteristic 2. Since R_1 is a finite commutative local ring, characteristic of R_1 is p^k for some prime p and some positive integer k. If p is an odd prime, then R_1 is of type (A).

Next assume that $p = 2$. Then $R_1/J(R_1) \cong GF(2^s)$ for some positive integer s. Since $R^*! \neq 1$, $J(R_1) \neq 0$. Suppose $k = 1$. If $J(R_1)^h \neq 0$ and $J(R_1)^{h+1} = 0$. Then $J(R_1)^h = J(R_1)^h/J(R_1)^{h+1}$ is a vector space over $GF(2^s)(\cong R_1/J(R_1))$, each $|J(R_1)^h|$ is a power of 2^s. More generally, since $|J(R_1)| = |J(R_1)/J(R_1)^2| \times \cdots \times |J(R_1)^h/J(R_1)^{h+1}|$ and since $J(R_1)^i/J(R_1)^{i+1}$ is a vector space over $GF(2^s)(\cong R_1/J(R_1))$ for each positive integer i, each $|J(R_1)^i/J(R_1)^{i+1}|$ is a power of 2^s, and so $|J(R_1)| = (2^s)^d$ for some non-negative integer d. If $s > 1$, then $J(R_1)^h$ contains at least two nonzero elements a and b. In this case, $1 + a$ and $1 + b$ are two distinct invertible elements of order 2, a contradiction. Hence we conclude that $s = 1$ and so $R_1/J(R_1) \cong GF(2)$. Therefore $R_1^* \cong 1 + J(R_1)$ by [6, Theorem XVIII.2]. By the observation above, $|R_1^*| = |1 + J(R_1)| = |J(R_1)|$ is a power of 2. R_1^* has precisely one element of order 2, R_1^* must be a cyclic group. In this case, R_1 is of type (D) or (E) by [1]. Next suppose that $k > 1$. Then $1 \neq -1$, and so -1 is an invertible element of order 2. Assume that R_1 contains a nonzero element a of square zero. Then there is a positive integer q such that $2^{q-1}a \neq 0$ and $2^q a = 0$. Then $1 + 2^{q-1}a$ is an invertible element of order 2, and hence $1 + 2^{q-1}a = -1$. Then $2 + 2^{q-1}a = 0$, and hence $2a = -2^{q-1}a^2 = 0$. Then $1 + a$ is an invertible element of order 2, and hence $1 + a = -1$. Therefore $a = -2$ and so $4 = a^2 = 0$. Consequently $4 = 0$ and 2 is the unique nonzero element of square zero. Since $(2R_1)^2 = 0$ and $2 \in 2R_1$, $2R_1 = \{0, 2\}$. Since $J(R_1)$ is nilpotent, $2R_1 J(R_1) \neq 2R_1$ and so $2R_1 J(R_1) = 0$. Hence $2R_1 (= \{0, 2\})$ is a vector space over $GF(2^s)(\cong R_1/J(R_1))$. Then $2 \geq 2^s$, and we conclude that $s = 1$. Thus $R_1/J(R_1) \cong GF(2)$, and therefore $R_1^* \cong 1 + J(R_1)$ by [6, Theorem XVIII.2]. Since $|R_1^*| = |1 + J(R_1)| = |J(R_1)|$ is a power of 2 and since R_1^* has precisely one element of order 2, R_1^* must be a cyclic group. In this case, R_1 is of type (B) or (C) by Gilmer's result [3, P. 447].

Conversely we shall show that if $R = R_1 \oplus \cdots \oplus R_m$, where all $R_2, \ldots, R_m$ are finite fields of characteristic 2 and R_1 is of one of types (A)-(E), then $R^*! \neq 1$. First suppose that R_1 is of type (A). Then $R_1/J(R_1) \cong GF(p^t)$ for some positive integer t. Since $J(R_1)$ is nilpotent, by [6, Theorem XXI.5] we have the exact sequence of groups: $1 \to 1 + J(R_1) \to R_1^* \to (R_1/J(R_1))^* \to 1$. Assume that $J(R_1)^h \neq 0$ and $J(R_1)^{h+1} = 0$. Then $|J(R_1)| = |J(R_1)/J(R_1)^2| \times \cdots \times |J(R_1)^h/J(R_1)^{h+1}|$. Since $J(R_1)^i/J(R_1)^{i+1}$ is a vector space over $GF(p^t)(\cong R_1/J(R_1))$ for each positive integer i, each $|J(R_1)^i/J(R_1)^{i+1}|$ is a power of p, and so $|J(R_1)| = p^d$ for some non-negative integer d. Since $R_1/J(R_1) \cong GF(p^t)$, $(R_1/J(R_1))^*$ is a cyclic group of order $p^t - 1$ and $|1 + J(R_1)| = p^d$, R_1^* has precisely one element of order 2, and so $R_1^* \neq \{1\}$ Next assume that R_1 is of one of types (B)-(E). Then R_1^* is a cyclic group by Gilmer's result [3, P. 447], and so $R_1^* \neq \{1\}$.

Hence in any case, we may assume that $R_1^*! = a$ for some unit a of order 2. Since $(R_2 \oplus \cdots \oplus R_m)^*$ is a group of odd order, we have $R^*! = a^{|(R_2 \oplus \cdots \oplus R_m)^*|} = a \neq 1$. □

Remark 1 *In* (C) *of Theorem 1, we have* $(4, 2x, x^2 - 2) = (2x, x^2 - 2)$, *because* $4 = -2(x^2 - 2) + (2x)x \in (2x, x^2 - 2)$.

3. Application to residually finite Dedekind domains

Gauss' generalization of Wilson's theorem is originally a result on the ring of integers. Toward the application of Theorem 1, we restate the assertion in Theorem 1 on some special class of Dedekind domains. A ring R is said to be residually finite if R/I is a finite ring for any nonzero ideal I of R. Clearly a ring of polynomials in one variable over a finite field is residually finite. The ring of algebraic integers in an algebraic number field is also residually finite by [3, Proposition 12.2.3].

First we state the following lemma without proof.

Lemma 2 *Let* R *be a residually finite Dedekind domain and suppose* P *is a prime ideal of* R *such that* $R/P \cong GF(2)$. *Then the following hold.*

(1) R/P^2 *is isomorphic to either* $Z/(4)$ *or* $GF(2)[x]/(x^2)$.

(2) R/P^3 *is isomorphic to one of the following:*

(A) $Z/(8)$;

(B) $Z[x]/(4,\ 2x,\ x^2 - 2)$;

(C) $GF(2)[x]/(x^3)$.

By Lemma 2 and Theorem 1, we obtain the following theorem.

Theorem 2 *Let* R *be a residually finite Dedekind domain and let* I *be a nonzero ideal of* R. *Then* $(R/I)^*! \neq 1$ *if and only if* I *is a finite product of distinct prime ideals* $P_1,\ P_2, \ldots,\ P_n$ *and an ideal* S *such that each* R/P_i *is a finite field of characteristic* 2, $P_i + S = R$ *and* S *satisfies one of the following:*

(i) $S = Q^k$ *for some positive integer* k, *where* Q *is a prime ideal such that* R/Q *is a finite field of characteristic* $p \neq 2$;

(ii) $S = P^2$ *where* P *is a prime ideal of* R *such that* $R/P \cong Z/(4)$;

(iii) $S = P^2$ *where* P *is a prime ideal of* R *such that* $R/P^2 \cong GF(2)[x]/(x^2)$;

(iv) $S = P^3$ *where* P *is a prime ideal of* R *such that* $R/P^3 \cong GF(2)[x]/(x^3)$;

(v) $S = P^3$ *where* P *is a prime ideal of* R *such that* $R/P^3 \cong Z[x]/(4,\ 2x,\ x^2 - 2)$.

We now give examples for some residually finite Dedekind domains.

Example 1 *Consider the polynomial ring* $R = GF(2)[x]$ *over* $GF(2)$. *Then* R *is a residually finite Dedekind domain of characteristic* 2. *Let* I *be a nonzero ideal of* R. *Then* $(R/I)^*! \neq 1$ *if and only if* $I = (f_1(x)f_2(x)\cdots f_n(x)x^k)$ *where* $f_1(x),\ f_2(x), \ldots, f_n(x)$ *are distinct irreducible polynomials with nonzero constants and* k *is* 2 *or* 3.

Example 2 *Consider* $R = Z[\sqrt[3]{2}]$. *Then* $(R/I)^*! \neq 1$ *if and only if* I *is one of the following:*

(i) $I = (\sqrt[3]{2})^\alpha P^\beta$ *where* $\alpha = 0$ *or* 1, β *is a positive integer and* P *is a prime ideal of* R *such that* $P \neq (\sqrt[3]{2})$.

(ii) $I = (2)$. *In this case,* $Z[\sqrt[3]{2}]/(2) \cong GF(2)[x]/(x^3)$ *and* $(Z[\sqrt[3]{2}]/(2))^*! = \overline{1 + \sqrt[3]{2}}$.

4. Wilson's theorem on rings of matrices over a finite commutative ring

Suppose that $n > 1$ and consider the ring $Mat_n(GF(q))$ of $n \times n$ matrices over $GF(q)$. We know that $Mat_n(GF(q))^* = GL(n,q)$. It is well known that the commutator subgroup of $GL(n,q)$ is $SL(n,q)$ unless $n = 2$ and $q = 2$ (see [7, Theorem 8.20]). Since $GL(n,q)/SL(n,q) \cong GF(q)^*$, $GL(n,q)/SL(n,q)$ has precisely one element of order 2 if and only if q is odd. Let us set $m = |GL(n,q)|$. It is well known that $m = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$. Hence $|SL(n,q)| = m/(q-1) = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-2})q^{n-1}$ is even, because $n > 1$. Hence by Corollary 1, if q is odd and if $GL(n,q) = \{a_1, \ldots, a_m\}$ then $a_1 \cdots a_m \in (-1)^{|SL(n,q)|}SL(n,q) = SL(n,q)$. If $n = 2$ and $q = 2$, then $GL(2,2) = SL(2,2)$. Summarizing the above consideration, we obtain the following:

Proposition 2 *Let* n *be a positive integer greater than* 1 *and* $R = Mat_n(GF(q))$ *and let* $R^* = \{a_1, \ldots, a_m\}$. *Then we have* $\det(a_1 \cdots a_m) = 1$ *in* $GF(q)$.

Remark 2 *Let* $R = Mat_2(GF(2))$. *Then* $R^* = GL(2,2) = SL(2,2) \cong S_3$ *and the commutator subgroup* $D(R^*)$ *of* R^* *is isomorphic to* A_3. *Hence* $R^*/D(R^*)$ *is a cyclic group of order 2. Let us consider concretely. Let* $R^* = \{a_1, a_2, a_3, a_4, a_5, a_6\}$. *Then* $a_1 \cdots a_6 \in \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$.

Let us generalize Proposition 2. Let R be a commutative ring, n a positive integer greater than 1, and T a subring of $Mat_n(R)$. Consider the restriction of determinant $\det : Mat_n(R) \to R$. to T^*, $\det|_{T^*} : T^* \to R^*$. Then $\det(T^*) \cong T^*/(Ker(\det|_{T^*}) = T^*/(Ker(\det) \cap T^*)$. Hence we have the following:

Lemma 3 *Let* R *be a finite commutative ring,* n *a positive integer greater than 1, and* T *a subring of* $Mat_n(R)$. *Let* $T^* = \{a_1, \cdots, a_m\}$. *Then* $\det(a_1 \cdots a_m) = (\det(T^*)!)^{|Ker(\det) \cap T^*|}$ *in* R^*.

Lemma 4 *Let* R *be a finite commutative local ring, and* n *a positive integer greater than 1. Then* $|Ker(\det) \cap Mat_n(R)^*|$ *is an even number.*

Proof Let $J(R)$ denote the Jacobson radical of R. Then the Jacobson radical of $Mat_n(R)$ is $Mat_n(J(R))$, and this is nilpotent. Hence by [6, Theorem XXI.5] we have the following exact sequence of groups: $1 \to 1 + Mat_n(J(R)) \to Mat_n(R)^* \to (Mat_n(R)/Mat_n(J(R)))^* \to 1$. Since $Mat_n(R)/Mat_n(J(R)) \cong Mat_n(R/J(R))$, $|Mat_n(R)^*| = |Mat_n(R/J(R))^*||J(R)|^{n^2}$. Also considering the exact sequence: $1 \to 1 + J(R) \to R^* \to (R/J(R))^* \to 1$, we have $|R^*| = |(R/J(R))^*||J(R)|$. Therefore we have $|Ker(\det) \cap Mat_n(R)^*| = |Mat_n(R)^*|/|R^*| = |Mat_n(R/J(R))^*||J(R)|^{n^2-1}/|(R/J(R))^*|$. Now let $R/J(R) = GF(q)$. Then this number equals to $(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})|J(R)|^{n^2-1}/(q-1) = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-2})q^{n-1}|J(R)|^{n^2-1}$. Since n is greater than 1, this number is even. □

Theorem 3 *Let R be a finite commutative ring, and n a positive integer greater than 1. Let $Mat_n(R)^* = \{a_1, \ldots, a_m\}$. Then $\det(a_1 \cdots a_m) = 1 \in R^*$.*

Proof We know that R is a direct sum of finite local rings, say $R = R_1 \oplus \cdots \oplus R_k$ where each R_i is a local ring. Let $Mat_n(R_i) = \{b_{i1}, b_{i2}, \ldots, b_{im(i)}\}$. Since the order of $(\det(Mat_n(R_i)^*))! \in R_i^*$ is less than or equal to 2, by Lemmas 3 and 4 we obtain $\det(b_{i1}b_{i2}\cdots b_{im(i)}) = (\det(Mat_n(R_i)^*)!)^{|Ker(\det)\cap Mat_n(R_i)^*|} = 1$ in R_i^*. Therefore $\det(a_1 \cdots a_m) = \prod_i \det(b_{i1}b_{i2}\cdots b_{im(i)})^{|Mat_n(R)|^*/|Mat_n(R_i)^*|} = 1 \in R^*$. □

References

[1] András, S.: A combinatorial generalization of Wilson's theorem, Australas. J. Combin. **49**, 265-272 (2011).

[2] Dicson, L.E.: History of the Theory of Numbers, Volume 1, Chelsea Publishing Company, New York, 1952.

[3] Gilmer, R.W.Jr.: Finite rings having a cyclic multiplicative group of units, Amer. J. Math. **85**, 447-452 (1963).

[4] Ireland, K. and Rosen, M.: A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, Vol. 84, Springer-Verlag, New York, 1981.

[5] Laššák, M.: Wilson's theorem in algebraic number fields, Math. Slovaca **50**, no. 3, 303-314 (2000).

[6] McDonald, B.R.: Finite Rings With Identity, Pure and Applied Mathematics, Vol. 28, Marcel Dekker, Inc., New York, 1974.

[7] Rotman, J.J.: An Introduction to the Theory of Groups, Fourth edition, Graduate Texts in Mathematics, Vol. 148, Springer-Verlag, New York, 1995.

[8] Tripathi, A.: A combinatorial proof of Wilson's theorem, Ars Combin. **80**, 201-204 (2006).