WILSON'S THEOREM: AN ALGEBRAIC APPROACH

PETE L. CLARK

Abstract. We discuss three algebraic generalizations of Wilson's Theorem: to (i) the product of the elements of a finite commutative group, (ii) the product of the elements of the unit group of a finite commutative ring, and (iii) the product of the nonzero elements of a finite commutative ring.

Introduction

We present several algebraic results inspired by Wilson's Theorem – for all prime numbers p, we have $(p-1)! \equiv -1 \pmod{p}$.

The standard proof of Wilson's Theorem proceeds by evaluating the product of all elements in the unit group $U(p)$ – that is, the group of nonzero residues modulo p under multiplication – by a pairing off argument. A natural algebraic generalization is to evaluate the product of all elements in a finite commutative group G. In §1 we state such a result – a theorem of G.A. Miller – and give two proofs. In §2 we consider the case of $U(n)$, the unit group of the ring $\mathbb{Z}/n\mathbb{Z}$, recovering a theorem of Gauss. Our treatment deliberately sidesteps the existence of primitive roots and so is more elementary than Gauss's approach, which is mentioned in §4. We then turn to the computation of the product of all elements of the unit group of a finite commutative ring, beginning in §3 with the case of a residue ring of a polynomial ring over a finite field – these rings stand in close, though not perfect, analogy to the rings $\mathbb{Z}/n\mathbb{Z}$ – and then treating in §5 the general case, a recent theorem of Hirano-Matsuoka. In §6 we compute the product of all nonzero elements of a finite ring. In §7 we briefly discuss Wilson semi-products, which are an algebraic generalization of $\frac{p-1}{2}!$ modulo p. In §8 we comment on the history, the literature and some other proofs of Wilson's Theorem.

The genesis of this paper was a conversation with my colleague Ted Shifrin on how the standard proofs of Miller's Theorem use structural results either for finite commutative groups or for finite-dimensional vector spaces over the field $\mathbb{Z}/2\mathbb{Z}$ and thus may not be accessible to an undergraduate student of group theory. I (truly!) believe that both proofs presented in §1 will be accessible to such students. The material of §2, §3 and §4 should be accessible to an undergraduate student who has seen groups and rings. We take pains to be as self-contained as possible, for instance giving not only a statement of the Chinese Remainder Theorem in the rings $\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}[t]$ but also a simpler proof than the standard one that exploits the finiteness of the residue rings. Many of the results of these sections are special cases of results in §5, so we are not aiming for logical efficiency but rather to understand and motivate these later results via accessible examples. The material of §5 and §6 should be accessible to students in a first graduate algebra course. Moreover we think that such students, in particular, will enjoy seeing interactions between the theories of finite commutative groups and of finite commutative rings. In §7 algebraic number theory appears in a rather breezy way: we do not attempt to be self-contained and some results are merely alluded to rather than stated precisely. Here we simply wish to convey connections and highlight some interesting open problems.

Notation and terminology: We denote by $\mathbb{Z}^+$ the positive integers $1, 2, 3, \ldots$. By a ring we will mean a commutative ring with a multiplicative identity. The additive group of a ring R will be denoted by $(R, +)$. For a ring R, we put

$$U(R) \coloneqq \{x \in R \mid \text{there is } y \in R \text{ such that } xy = 1\},$$

the **unit group** of R. We also put

$$U(n) \coloneqq (\mathbb{Z}/n\mathbb{Z})^\times,$$

the unit group modulo n. A zero divisor in a ring R is an element $x \in R$ for which there is $y \in R^\bullet$ with $xy = 0$. Except in the zero ring, 0 is always a zero divisor; any other zero divisor is called proper. An integral domain is a nonzero ring without proper zero divisors.

1. Wilson's Theorem in a Finite Commutative Group

1.1. **The problem.** Let $(G, \cdot)$ be a finite commutative group, with identity element e. Put

$$S \coloneqq \prod_{x \in G} x,$$

the product of all elements of G. Can we determine S?

Example 1.1. *Suppose $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$ is cyclic of order n. Then*

$$S \equiv 1 + \cdots + n \equiv \frac{n(n+1)}{2} \pmod{n}.$$

- *If n is odd then $\frac{n+1}{2} \in \mathbb{Z}$ and $S \equiv n\left(\frac{n+1}{2}\right) \equiv 0 \pmod{n}$. So $S = 0$.*
- *If n is even then $\frac{n(n+1)}{2}$ is not divisible by n, so $S \neq 0$. But $2S = n(n+1) = 0$, so S has order 2. The unique order 2 element of G is $\frac{n}{2}$, so $S = \frac{n}{2}$.*

Example 1.2. *Let p be an odd prime, and let $U(p)$ be the multiplicative group of nonzero elements of the field $\mathbb{Z}/p\mathbb{Z}$. As in any field, if $x^2 = 1$ then $0 = x^2 - 1 = (x+1)(x-1)$, so $x = \pm 1$. For every element $x \in U(p)$ with $x^2 \neq 1$, we have that x and x^{-1} are distinct elements of G and thus cancel each other out in the product. It follows that $S = 1 \cdot (-1) = -1$.*

The unit group $U(2) = U(\mathbb{Z}/2\mathbb{Z})$ has a single element $1 = -1$. We deduce:

Theorem 1.3 (Wilson's Theorem)**.** *For any prime p, we have $(p-1)! \equiv -1 \pmod{p}$.*

1.2. **Statement of the result.** We now state the general case, a result of Miller [Mi03].

Theorem 1.4. *Let G be a finite commutative group, and put $S \coloneqq \prod_{x \in G} x$.*
a) If G has no element of order 2, then $S = e$.
b) If G has exactly one element t of order 2, then $S = t$.
c) If G has at least two elements of order 2, then $S = e$.

The elements of G of order greater than 2 come in mutually inverse pairs $x \neq x^{-1}$, so the product over all such x is e. Thus $S = \prod_{x \in G[2]} x$, where $G[2]$ is the subset of elements of order at most two. Observe that $G[2]$ is a subgroup of G:

$$x = x^{-1}, y = y^{-1} \implies (xy)^{-1} = y^{-1}x^{-1} = yx = xy.$$

Although we don't need it, it seems remiss not to mention the following simple result:

Lemma 1.5. *Let G be a group in which each non-identity element has order 2. Then G is commutative.*

Proof. Let $x, y \in G$. Since $x^2 = y^2 = e$ we have $x^{-1} = x$ and $y^{-1} = y$. Multiplying the equation $e = (xy)^2 = xyxy$ on the left by x^{-1} and on the right by y^{-1} gives $xy = x^{-1}y^{-1} = yx$. □

Thus we have reduced Theorem 1.4 to the case $G = G[2]$. We will give two treatments of this case.

1.3. **First proof of Theorem 1.4.**

Lemma 1.6. *Let G be a group in which each non-identity element has order 2. Let H be a subgroup of G, and let $y \in G \setminus H$. Then the set*

$$\{h \in H\} \cup \{hy \mid h \in H\}$$

is a subgroup of G order twice the order of H.

Proof. This comes out immediately, as we invite the reader to check. □

Lemma 1.7. *Let G be a finite group in which each non-identity element has order 2.*
a) The order of G is 2^k for some $k \geq 0$.
b) If G has order greater than 1, it admits a subgroup H of order 2^{k-1}.

Proof. We prove both parts at once by an inductive argument. Put $H_0 = \{e\}$. If $G = H_0$, we're done. Otherwise there is $x_1 \in G \setminus H_0$, and by Lemma 1.6, $H_1 = \{e, x_1\}$ is a subgroup of order 2. If $G = H_1$, we're done. Otherwise there i $x_2 \in G \setminus H_1$, and applying Lemma 1.6 we get that $H_2 = \{h \in H_1\} \cup \{x_2 h \mid h \in H_1\}$ has order 4. Continuing in this manner, we suppose that H_n is a proper subgroup of G of order 2^n. Then we can continue the process, choosing $x_{n+1} \in G \setminus H_n$ and putting $H_{n+1} = \{h \in H_n\} \cup \{x_{n+1} h \mid h \in H_n\}$, so H_{n+1} is a subgroup of order 2^{n+1}. Since G is finite, there must be some n such that $H_n = G$, completing the proof. □

Now we give our first proof of Theorem 1.4: above we reduced to the case in which $G = G[2]$ is a finite commutative group in which each nonidentity element has order 2. Put $S \coloneqq \prod_{x \in G} x$. Then:
(i) If G has no elements of order 2, then G is trivial and $S = e$.
(ii) If G has exactly one element t of order 2, then $G = \{e, t\}$ and $S = et = t$.
(iii) Suppose G has at least two elements of order 2. By Lemmas 1.6 and 1.7, the group G has order 2^k for some $k \geq 2$, there is a subgroup H of order 2^{k-1} and an element $y \in G \setminus H$ such that G is the disjoint union of $\{h \in H\}$ and $\{yh \mid h \in H\}$. Thus

$$\prod_{x \in G} x = \prod_{h \in H} h \prod_{h \in H} yh = \prod_{h \in H} yh^2 = \prod_{h \in H} y = y^{2^{k-1}} = (y^2)^{2^{k-2}} = e^{2^{k-2}} = e.$$

1.4. **Second proof of Theorem 1.4.** We follow Vandiver-Weaver [VW58] and Saucier [Sa18].

Lemma 1.8. *Let G be a group in which each nonidentity element has order 2, and let a be a nonidentity element of G. Then the map*

$$\iota_a : G \to G, \ x \mapsto ax^{-1}$$

is a fixed point free involution of G: i.e., for all $x \in G$ we have $\iota_a(x) \neq x$ and $\iota_a(\iota_a(x)) = x$.

Proof. If $x \in G$ then we have

$$\iota_a(\iota_a(x)) = a(ax^{-1})^{-1} = e.$$

If for $x \in G$ we have $x = \iota_a(x) = ax^{-1}$ then $e = x^2 = a$:, a contradiction. □

Now let G be finite commutative: again we may assume that G has order $n > 1$ and that every nonidentity element of G has order 2. Let a be a nonidentity element of G. Lemma 1.8 implies that $n = 2m$ is even and that we may order the elements of G as $x_1, ..., x_{2m}$ such that for all $1 \leq i \leq m$ we have $x_{2i-1} x_{2i} = a$. Then

$$S = \prod_{1 \leq i \leq m} x_{2i-1} x_{2i} = a^m.$$

Case (i): Suppose $m = 1$; equivalently, a is the unique element of order 2. Then $S = a^1 = a$.
Case (ii): Supose $m = 2M$ is even. Then $S = a^{2M} = (a^2)^M = e$.
Case (iii) Suppose $m = 2M + 1$ with $M \geq 1$. Then we get $S = a^{2M+1} = (a^2)^M a = a$. On the other hand, since $m \geq 2$ there is $b \in G \setminus \{1, a\}$, and the same argument shows $S = b^{2M+1} = b$ and thus $a = b$. This contradiction shows that this case cannot occur.[1]

[1]This was no surprise, since Lemma 1.7 implies that m is a power of 2. But we are giving an independent proof.

1.5. **The dichotomy given by an order 2 element in a finite commutative group.** Let G be a finite commutative group, and let $t \in G$ be an element of order 2. By Theorem 1.4, the product $S = \prod_{x \in G} x$ is *either* e or t. To show $S = e$ we need to find another element of order 2. To show $S = t$ we need to show there are no other elements of order 2. This is an interesting dichotomy.

In particular, let $n \in \mathbb{Z}^+$, and let $G = U(n)$ be the unit group of $\mathbb{Z}/n\mathbb{Z}$. If $n \leq 2$ then $U(n) = \{1\}$, so $\prod_{x \in U(n)} x = 1$. If $n \geq 3$ then -1 is an order 2 element of $U(n)$, and so we get $\prod_{x \in U(n)} x = \{\pm 1\}$.

When n is prime, then (cf. Example 1.2) the equation $x^2 = 1$ has only ± 1 as solutions. But $x^2 = 1$ may have more than two solutions in $\mathbb{Z}/n\mathbb{Z}$ for composite n: e.g. if $n = 8$ then $\prod_{x \in U(8)} x = 1 \cdot 3 \cdot 5 \cdot 7 = 105 = 1$ in $\mathbb{Z}/8\mathbb{Z}$, and $1^2 = 3^2 = 5^2 = 7^2 = 1$ in $\mathbb{Z}/8\mathbb{Z}$, so $U(8)$ has three elements of order 2.

For all n, Gauss determined the sign in $\prod_{x \in U(n)} x = \pm 1$. We turn to this next.

2. Gauss's Generalization of Wilson's Theorem

Let $m, n \in \mathbb{Z}^+$. There is a homomorphism of rings

$$\Phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, x \mapsto (x \pmod m, x \pmod n).$$

The kernel of Φ is the set of integers x such that $x \equiv 0 \pmod m$ and $x \equiv 0 \pmod n$, i.e., the set of integers divisible by the least common multiple $\operatorname{lcm}(m, n)$, and thus we get an injective homomorphism

$$\mathbb{Z}/\operatorname{lcm}(m, n)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Now $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has mn elements, so we have a bijection iff $\operatorname{lcm}(m, n) = mn$ iff $\gcd(m, n) = 1$. An easy induction extends this to the following result.

Proposition 2.1 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_r \in \mathbb{Z}^+$ be such that $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j < r$. Then we have an isomorphism of rings*

$$\mathbb{Z}/m_1 \cdots m_r\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/m_i\mathbb{Z},\ x \mapsto (x \pmod{m_1}, \ldots, x \pmod{m_r}).$$

For rings $R_1, \ldots, R_r$, let $\prod_{i=1}^r R_i$ denote the product $R_1 \times R_2 \times \ldots \times R_r$, a ring under coordinatewise addition and multiplication. For $(x_1, \ldots, x_r) \in \prod_{i=1}^r R_i$, we have $(x_1, \ldots, x_r) \in U(\prod_{i=1}^r R_i)$ iff $x_i \in U(R_i)$ for all $1 \leq i \leq r$. It follows that

$$U(\prod_{i=1}^r R_i) = \prod_{i=1}^r U(R_i), \tag{1}$$

where on the right hand side we have a direct product of commutative groups.

Theorem 2.2 (Gauss)**.** *Let $n \in \mathbb{Z}^+$, and put $G_n \coloneqq \prod_{x \in U(n)} x$.*
a) If $n = 4$ or is of the form p^a or $2p^a$ for an odd prime p, then $G_n = -1$.
b) Otherwise we have $G_n = 1$.

Proof. Recall that for any $x \in \mathbb{Z}$, $x \pmod n$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(x, n) = 1$.[2]
Write $n = 2^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ with $a_1 \geq 0$,$a_2, \ldots, a_r \geq 1$, so by the Chinese Remainder Theorem and (1),

$$U(n) \cong U(2^{a_1}) \times \prod_{i=2}^r U(p_i^{a_i}). \tag{2}$$

(We allow $r = 1$, in which case we mean $n = 2^{a_1}$.)
Step 1: As above we may assume $n > 2$, so $-1 \in U(n)[2]$ and by Theorem 1.4 $\prod_{x \in U(n)} x = -1$ if $U(n)[2] = \{\pm 1\}$ and $\prod_{x \in U(n)} x = 1$ if $U(n)[2] \supsetneq \{\pm 1\}$. Moreover if $a_1 = 1$ then $U(n) \cong U(2) \times U(n/2) \cong U(n/2)$, and the result is the same for n as for $n/2$. Thus we may assume that n is odd or is divisible by 4.

[2]For instance, by the Eulidean algorithm if $\gcd(x, n) = 1$ then there are integers a, b such that $ax + bn = 1$, and thus $(a \pmod n) = (x \pmod n)^{-1}$. If $\gcd(x, n) = d > 1$, then reducing $xa \pmod n$ modulo d gives $0 \equiv xa \equiv 1 \pmod d$, a contradiction.

Step 2: Suppose $n = p^a$ for a prime $p > 2$ and $a \in \mathbb{Z}^+$. Let $x \in U(p^a)[2]$. If in $\mathbb{Z}/p^a\mathbb{Z}$ both $x+1$ and $x-1$ were multiples of p, then $(x+1)-(x-1) = 2$ would be too, contradicting $p > 2$. So either $x+1$ is not a multiple of p — in which case it is a unit, so $(x+1)(x-1) = 0$ implies $x-1 = 0$ and $x = 1$ — or $x-1$ is not a multiple of p, and similarly we get $x+1 = 0$ and $x = -1$.
Step 3: Suppose $a_1 \geq 3$. Then $1 + 2^{a_1-1} \in U(2^{a_1}) \setminus \{\pm 1\}$, so $U(2^{a_1})$ has more than one element of order 2. Since $U(2^{a_1})$ is isomorphic to a subgroup of $U(n)$, also $U(n)$ has more than one element of order 2.
Step 4: Suppose $a_1 = 2$. If $r = 1$ – i.e., $n = 4$ – then $U(n) = \{\pm 1\}$ and the result is clear. Otherwise there is $x \in U(n)$ with $x \equiv 1 \pmod 4$ and $x \equiv -1 \pmod{p_i^{a_i}}$ for all $i \geq 2$, which gives an element of order 2 other than ± 1.
Step 5: The last case is $r \geq 3$, and there is $x \in U(n)$ with $x \equiv 1 \pmod{p_2^{a_2}}$, $x \equiv -1 \pmod{p_i^{a_i}}$, which gives an element of order 2 other than ± 1. □

3. The Generalized Wilson Theorem in Polynomial Rings

The kinship between $\mathbb{Z}$ and the polynomial ring $\mathbb{Z}/p\mathbb{Z}[t]$ is a rich theme in algebra and number theory. We will see a glimmer of this now, by giving the analogue of Theorem 2.2 over $\mathbb{Z}/p\mathbb{Z}[t]$ for $p > 2$.

Let $n(t) \in \mathbb{Z}/p\mathbb{Z}[t]$ be a polynomial of positive degree, and put

$$U(n(t)) \coloneqq U(\mathbb{Z}/p\mathbb{Z}[t]/(n(t))).$$

We will compute

$$G_{n(t)} \coloneqq \prod_{x \in U(n(t))} x.$$

The rings $\mathbb{Z}/p\mathbb{Z}[t]/(n(t))$ all have characteristic $p > 2$, so $-1 \neq 1$ Theorem 1.4 gives $G_{n(t)} \in \{\pm 1\}$.

In the ring $\mathbb{Z}/p\mathbb{Z}[t]$ one can perform division with remainder and thus obtain a Euclidean algorithm, with the usual consequence that elements factor uniquely into products of prime elements, which here are irreducible polynomials. Thus

$$n(t) = p_1(t)^{a_1} \cdots p_r(t)^{a_r},$$

with $p_1(t), \ldots, p_r(t)$ distinct monic irreducible polynomials. The Chinese Remainder Theorem adapts to this context: if $m(t)$, $n(t)$ are coprime polynomials (they have no common divisor of positive degree), then their least common multiple is their product $m(t)n(t)$, so the kernel of the natural map

$$\mathbb{Z}/p\mathbb{Z}[t] \to \mathbb{Z}/p\mathbb{Z}[t]/(m(t)) \times \mathbb{Z}/p\mathbb{Z}[t]/(n(t))$$

is $m(t)n(t)$, and we get an injective homomorphism

$$\mathbb{Z}/p\mathbb{Z}[t]/(m(t)n(t)) \to \mathbb{Z}/p\mathbb{Z}[t]/(m(t)) \times \mathbb{Z}/p\mathbb{Z}[t]/(n(t)). \tag{3}$$

If $f(t)$ has degree d, then $\mathbb{Z}/p\mathbb{Z}[t]/(f(t))$ has order p^d. If $m(t)$ has degree d_m and $n(t)$ has degree d_n, then $m(t)n(t)$ has degree $d_m + d_n$, so both $\mathbb{Z}/p\mathbb{Z}[t]/(m(t)n(t))$ and $\mathbb{Z}/p\mathbb{Z}[t]/(m(t)) \times \mathbb{Z}/p\mathbb{Z}[t]/(n(t))$ have order $p^{d_m+d_n}$, and as above, the homomorphism (3) is an isomorphism. Induction gives

$$\mathbb{Z}/p\mathbb{Z}[t]/(n(t)) \xrightarrow{\sim} \prod_{i=1}^{r} \mathbb{Z}/p\mathbb{Z}[t]/(p_i(t)^{a_i})$$

hence

$$U(n(t)) \cong \prod_{i=1}^{r} U(p_i(t)^{a_i}).$$

Theorem 3.1. *(Li-Sha* [LS17, Thm. 3.1]*) Let $p > 2$ be a prime, and let $n(t) \in \mathbb{Z}/p\mathbb{Z}[t]$ be monic of positive degree. If $n(t)$ is a power of an irreducible polynomial, then $G_{n(t)} = -1$. Otherwise $G_{n(t)} = 1$.*

Proof. We invite the interested reader to check that the method of proof of Theorem 2.2 applies. □

Example 3.2. *For $n \in \mathbb{Z}^+$ consider the ring $R_n := \mathbb{Z}/2\mathbb{Z}[t]/(t^n)$, of characteristic 2 and order 2^n. The units are represented by polynomials of degree less than n having constant term 1 (rather than 0). Thus $U(R_n)$ has order 2^{n-1}.*
a) $(n = 1)$: We have $R_1 = \mathbb{Z}/2\mathbb{Z}$, so $U(R_1)$ is the trivial group.
b) $(n = 2)$: We have $\prod_{x \in U(R_2)} x = 1 \cdot (t + 1) = t + 1$.
c) $(n = 3)$: We have

$$\prod_{x \in U(R_3)} x = 1(t+1)(t^2+1)(t^2+t+1) = t^5 + 2t^4 + 3t^3 + 3t^2 + 2t + 1 = t^2 + 1.$$

It follows from Theorem 1.4 (see also Theorem 5.2) that $U(R_3)$ is generated by $t + 1$.
d) $(n \geq 4)$: If $\frac{n}{2} \leq k < n$ we have $2k \geq n$, so $(t^k + 1)^2 = t^{2k} + 1 = t^n t^{2k-n} + 1 = 1$. This exhibits $\lfloor \frac{n}{2} \rfloor \geq 2$ order 2 elements of $U(R_n)$, so $\prod_{x \in U(R_n)} x = 1$.

In fact the paper [LS17] treats the case of polynomials defined over any finite field $\mathbb{F}$. When $\mathbb{F}$ has odd cardinality, Theorem 3.1 and its proof hold verbatim. But as Example 3.2 suggests, the case of finite fields of even cardinality is more complicated. In turn, their result is a special case of a result of Hirano-Matsuoaka that we will discuss later: Theorem 5.15.

4. Interlude on cyclicity

Our approach to Gauss's Generalized Wilson Theorem is not the same as Gauss's. Rather Gauss went farther by determining the exact structure of $U(n)$ for all n. In view of (2) the essential case is that of a prime power.

Theorem 4.1 (Gauss)**.**
a) For every odd prime power p^a, we have $U(p^a) \cong (\mathbb{Z}/p^{a-1}(p-1)\mathbb{Z}, +)$.
b) For all $a \geq 3$, we have $U(2^a) \cong (\mathbb{Z}/2^{a-2}\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$.

The proof of Theorem 4.1 may be found in many number theory texts, e.g. [C-NT]. We will not give it here. But we discuss some consequences.

From Theorem 4.1 and Example 1.1 one deduces Theorem 2.2. One also determines when $U(n)$ is cyclic: in fact, for all $n \geq 3$, this occurs iff $\prod_{x \in U(n)} x = -1$. In the classical terminology, a generator of $U(n)$ is called a **primitive root**, so we find that primitive roots exist modulo n iff $n \in \{1, 2, 4\}$; n is an odd prime power; or n is twice an odd prime power. This is a basic and useful result.

But the analogue of Theorem 4.1a) in the context of polynomial rings fails:

Proposition 4.2. *For p a prime number and $n \geq 4$, the unit group $U(t^n)$ of $\mathbb{Z}/p\mathbb{Z}[t]/(t^n)$ is not cyclic.*

Proof. Let R be the ring $\mathbb{Z}/p\mathbb{Z}[t]/(t^n)$. We claim $1 + t^{n-1}$ and $1 + t^{n-2}$ generate distinct order p subgroups $U(t^n)$. Since $n \geq 4$, we have $2n - 4 \geq n$ and thus $t^{2n-4} = 0$ in R. Thus

$$(1 + t^{n-2})^2 = 1 + 2t^{n-2} + t^{2n-4} = 1 + 2t^{n-2}.$$

By induction, for all $j \in \mathbb{Z}^+$ we have

$$(1 + t^{n-2})^j = 1 + jt^{n-2}.$$

Similarly, for all $j \in \mathbb{Z}^+$ we have

$$(1 + t^{n-1})^j = 1 + jt^{n-1}.$$

□

The reader might like to try to show that for all $p > 2$, the group $U(\mathbb{Z}/p\mathbb{Z}[t]/(t^2))$ is cyclic and $U(\mathbb{Z}/p\mathbb{Z}[t]/(t^3))$ is not. Later we will meet the definitive result in this area. The following result shows that the lack of cyclicity is just the tip of the iceberg.

Theorem 4.3. *(*[R, Prop. 1.6]*) Let $\mathbb{F}$ be a finite field of characteristic p, let $f \in \mathbb{F}[t]$ be an irreducible polynomial, let $a \in \mathbb{Z}^+$. The number of elements of order p in $U(\mathbb{F}[t]/(f^a))$ approaches infinity with a.*

The exact structure of $U(\mathbb{F}[t]/(f^a))$ *is* known, a result of Smith-Gallian [SG85]. Even the statement is rather complicated, and we will not reproduce it here.

5. Wilson's Theorem in a Finite Ring

Let R be a finite ring. In this section we will compute

$$u(R) := \prod_{x \in U(R)} x,$$

recovering a recent theorem of Hirano-Matsuoka [HM13].

5.1. **Group Theoretic Preliminaries.**

For a finite commutative group G and a prime number p, let G_p be the subgroup of $x \in G$ of order a power of p. We call G_p the **p-primary component** of G.

Theorem 5.1 (Structure Theorem for Finite Commutative Groups)**.**
Let G be a finite commutative group, of order $n = p_1^{a_1} \cdots p_r^{a_r}$.
a) We have $G = \prod_{i=1}^r G_{p_i}$, and for all $1 \leq i \leq r$, we have $\#G_{p_i} = p_i^{a_i}$.
b) For all $1 \leq i \leq r$, G_{p_i} is isomorphic to a direct sum of finite cyclic p_i-groups: there are positive integers s_i and $e_{i,1} \leq e_{i,2} \leq \ldots \leq e_{i,s_i}$ such that

$$G_{p_i} \cong \prod_{j=1}^{s_i} (\mathbb{Z}/p^{e_{i,j}}\mathbb{Z}, +).$$

c) The integers $\{s_i\}_{1 \leq i \leq r}$, $\{e_{i,j}\}_{1 \leq j \leq s_i}$ are independent of the chosen isomorphisms.

Proof. See e.g. [C-NT, Appendix B, §5]. □

Theorem 5.2. *For a finite commutative group G, the following are equivalent:*
(i) G is cyclic.
(ii) For all primes p dividing the order of G, G_p is cyclic.
(iii) For all primes p dividing the order of G, G_p has exactly one subgroup of order p (equivalently, there are exactly p elements $x \in G$ such that $x^p = e$).

Proof. (i) $\iff$ (ii): A product $\prod_{i=1}^r G_i$ of finite groups is cyclic iff each G_i is cyclic and for all $1 \leq i < j \leq n$, G_i and G_j have coprime order.
(ii) $\implies$ (iii): a cyclic group of order n has a unique subgroup of each order $d \mid n$.
(iii) $\implies$ (ii): Let p divide the order of G. By Theorem 5.1 we have

$$G_p \cong \prod_{j=1}^{s} (\mathbb{Z}/p^{e_j}\mathbb{Z}, +).$$

So $s = 1$ iff G_p is cyclic iff G_p has a unique subgroup of order p. □

Remark 5.3. *It is rather easy to establish the decomposition $G = \prod G_p$, and this is the first step of the proof of Theorem 5.1. The second step is to show that a finite commutative p-group is cyclic iff it has a unique subgroup of order p.*

Lemma 5.4.
Let $f : G \to H$ be a homomorphism of finite commutative groups, and let p be a prime number.
a) We have $f(G_p) \subset H_p$. Thus there is a well-defined homomorphism

$$f_p = f|_{G_p} : G_p \to H_p.$$

b) If f is surjective with kernel of order prime to p, then $f_p : G_p \xrightarrow{\sim} H_p$.

Proof. a) This is left to the reader.
b) Let K be the kernel of f. In general the order of G_p is the largest power of p dividing the order of G. In this case, the order of G is the order of H times the order of K, which is prime to p, so the largest power of p dividing the order of G is equal to the largest power of p dividing the order of H, so G_p and H_p have the same order. Moreover, the kernel $K \cap G_p$ of f_p is $K \cap G$ consists of elements of order

both prime to p and a power of p. So it is trivial, and $f_p : G_p \to H_p$ is an injective homomorphism between finite groups of equal order: thus it is an isomorphism. □

5.2. **Ring Theoretic Preliminaries.**

Theorem 5.5 (Lagrange)**.** *Let F be a field, and let $f \in F[t]$ be a nonzero polynomial of degree d. Then the set $\{x \in F \mid f(x) = 0\}$ has size at most d.*

Proof. This is a quick consequence of the Root Factor Theorem from high school algebra: if $f(x) = 0$ then $f(t) = (t - x)g(t)$ for some polynomial g of degree $d - 1$. □

Corollary 5.6. *Let G be a finite subgroup of the group of units of a field F. Then G is cyclic.*

Proof. Let p be a prime dividing the order of G. By Lagrange's Theorem the polynomial $t^p - 1$ has at most p roots in F, so there are at most p elements $x \in G$ such that $x^p = 1$ We apply Theorem 5.2. □

Lemma 5.7. *a) Let $R_1, \ldots, R_r$ be rings. Then the characteristic of $R = \prod_{i=1}^r R_i$ is the least common multiple of the characteristics of R.*
b) If R is a finite ring, the characteristic of R divides the order of R.

Proof. a) This is left to the reader. b) The characteristic of R is the order of 1 in the additive group $(R, +)$. Now we use another theorem of Lagrange: the order of a subgroup of a finite group divides the order of the group. □

Theorem 5.8 (Primary Decomposition Theorem)**.** *Let R be a nonzero finite ring.*
a) The following are equivalent:
*(i) R is **local**: the set $\mathfrak{m} = R \setminus U(R)$ of nonunits forms an ideal of R, which is then necessarily the unique maximal ideal of R.*
*(ii) R is **primary**: every zero divisor $x \in R^\bullet$ is nilpotent: $x^n = 0$ for some $n \in \mathbb{Z}^+$.*
b) If R is local, its order is a prime power p^a. There are integers $b, c \leq a$ such that R has characteristic p^b, $\mathfrak{m}$ has order p^c and $R/\mathfrak{m}$ is a finite field of order p^{a-c}.
c) For every finite ring R, there are nonzero local rings $R_1, \ldots, R_r$ such that $R \cong \prod_{i=1}^r R_i$. The ring R has precisely r maximal ideals.

Proof. A finite ring R is Artinian: it satisfies the descending chain condition on ideals. Part c) is the finite case of a structure theorem for Artinian rings [C-CA, Thm. 8.35]. Moreover, in a local Artinian ring R the maximal ideal is precisely the set of nilpotent elements of R [C-CA, Thm. 8.31], so a local Artinian ring is primary. Conversely no product $\prod_{i=1}^r R_i$ of nonzero rings is primary: the element $e_1 = (1, 0, \ldots, 0)$ is a proper zero divisor with $e_1^2 = e_1$, so is not nilpotent. So a primary Artinian ring is local. It remains to show that a finite local ring $(R, \mathfrak{m})$ has prime power order, from which the rest of part b) follows. The key idea is that there is some $N \in \mathbb{Z}^+$ such that $\mathfrak{m}^N = (0)$ [C-CA, Thm. 8.31]. The quotient $R/\mathfrak{m}$ is a finite field of prime power order q, say. But then moreover for all $0 \leq i \leq N - 1$ the quotient $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is naturally a vector space over $R/\mathfrak{m}$, hence has order a power of q. Therefore R has order a product of powers of q, hence a prime power. □

Let R and S be nonzero rings, and let $f : R \to S$ be a homomorphism. Then $f(U(R)) \subset U(S)$, so there is an induced map

$$U(f) : U(R) \to U(S), x \mapsto f(x)$$

which is a homomorphism of groups.

Suppose f is surjective. In general, $U(f)$ need not be surjective: the problem is of course that for $v \in U(S)$, although there is $x \in R$ such that $f(x) = v$, there may not exist any such x that is a unit. For instance let $p > 3$ be a prime and consider the quotient map $f : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Then $2 \pmod p \in U(p)$, but the units of $\mathbb{Z}$ are precisely ± 1, neither of which is congruent to 2 modulo p.

On the other hand, in the above situation, at least x cannot be a nilpotent element (unless S is the zero ring, a trivial case): if $x^n = 0$, then also $v^n = f(x)^n = f(x^n) = f(0) = 0$, so v is nilpotent. But if w is such that $vw = 1$, then $1 = v^n w^n = 0 w^n = 0$, contradiction. By Theorem 5.8, in any finite local ring every non-nilpotent element is a unit, and thus we get the following result.

Lemma 5.9. *Let R be a finite local ring, and let $f : R \to S$ be a surjective ring homomorphism. Then $U(f) : U(R) \to U(S)$ is surjective.*

Remark 5.10. *More generally, let $f : R \to S$ be a surjective ring homomorphism for which the kernel is contained in all but finitely many maximal ideals of R. Then the induced homomorphism $U(f) : U(R) \to U(S)$ is surjective* [C-CA, Thm. 4.32].

5.3. **Wilson's Theorem in a Finite Ring of Odd Order.**

Theorem 5.11. *Let R be a finite ring of odd order. Then:*
a) If R is local, we have $u(R) = \prod_{x \in U(R)} x = -1$.
b) If R is not local, we have $u(R) = \prod_{x \in U(R)} = 1$.

Proof. a) This is a generalization of the fact that $\prod_{x \in U(p^a)} x = -1$, and we can use the same argument: since R has odd order, it has odd characteristic and thus $-1 \neq 1 \in U(R)[2]$. Let $x \in U(R)[2]$, i.e., $x^2 = 1$. If $x+1, x-1$ both lie in $\mathfrak{m}$ then so does $(x+1)-(x-1) = 2$, contradicting the fact that R has odd characteristic. If $x+1 \in U(R)$, then $(x+1)(x-1) = 0$ implies $x-1 = 0$ so $x = 1$; similarly, if $x-1 \in U(R)$, then $x = -1$. By Theorem 1.4 we have $\prod_{x \in U(R)} x = -1$.
b) If R is not local, Theorem 5.8 gives $R \cong \prod_{i=1}^r R_i$ with $r \geq 2$. Then $U(R) \cong \prod_{i=1}^r U(R_i)$ has more than one element of order 2 and $\prod_{x \in U(R)} x = 1$. □

Remark 5.12. *Here is an alternate proof that $u(R) = -1$ when R is odd order local, say of order p^a for an odd prime p, with $\mathfrak{m} = R \setminus U(R)$. The map $U(q) : U(R) \to U(R/\mathfrak{m})$ is a surjection with kernel $1 + \mathfrak{m}$ a p-group, so by Lemma 5.4 we have $U(q)_2 \cong U(R/\mathfrak{m})_2$. Hence $U(q)[2] \cong U(R/\mathfrak{m})[2] = \{\pm 1\}$, so $u(R) = -1$.*

5.4. **Wilson's Theorem in a Finite Ring: The General Case.**

Suppose R is a finite local ring of even characteristic. Let $\mathfrak{m} = R \setminus U(R)$ be the maximal ideal of R. By the Primary Decomposition Theorem there are $0 \leq b < a$ such that R has order 2^a and $\mathfrak{m} = R \setminus U(R)$ has order 2^b. Then $R/\mathfrak{m}$ is a field of order 2^{a-b}, so $U(R/\mathfrak{m})$ is cyclic of odd order $2^{a-b} - 1$. By Lemma 5.9, the quotient map $R \to R/\mathfrak{m}$ induces a surjective homomorphism on unit groups

$$U(q) : U(R) \to U(R/\mathfrak{m}).$$

The kernel of $U(q)$ is $1+\mathfrak{m}$, of order 2^b. So for any prime $p > 2$, by Lemma 5.4b) we get an isomorphism $U(R)_p \xrightarrow{\sim} U(R/\mathfrak{m})_p$. By Corollary 5.6 the group $U(R/\mathfrak{m})$ is cyclic, hence so is its subgroup $U(R/\mathfrak{m})_p$ and thus $U(R)_p$ is also cyclic. Applying Theorem 5.2 we find that $U(R)$ is cyclic iff $U(R)_2$ is cyclic iff $U(R)$ has at most one element of order 2. Moreover, $U(R) = R \setminus \mathfrak{m}$ has size $2^a - 2^b$ hence has odd order iff $b = 0$ iff $\mathfrak{m} = (0)$ iff R is a finite field. Thus:

Proposition 5.13. *Let R be a finite local ring of even order. Then:*
a) If R is a field, then $U(R)[2] = \{1\}$ and $u(R) = 1$.
b) If R is not a field and $U(R)$ is cyclic, then $U(R)[2] = \{1, t\} \supsetneq \{1\}$ and $u(R) = t$.
c) If R is not a field and $U(R)$ is not cyclic, then $U(R)[2]$ has more than two elements and $u(R) = 1$.

Thus, whereas in the odd order case we were able to bypass the issue of cyclicity of the unit group, in the even order local case we have reduced the problem to knowing when the unit group is cyclic. Fortunately there is a beautiful answer.

Theorem 5.14. *a) (Gilmer* [Gi63]*) Let R be a finite, local ring. Then $U(R)$ is cyclic iff R is isomorphic to one of the following rings:*
(A) A finite field $\mathbb{F}$.
(B) $\mathbb{Z}/p^a\mathbb{Z}$ for an odd prime number p and $a \in \mathbb{Z}^+$.
(C) $\mathbb{Z}/4\mathbb{Z}$.
(D) $\mathbb{Z}/p\mathbb{Z}[t]/(t^2)$ for a prime number p.
(E) $\mathbb{Z}/2\mathbb{Z}[t]/(t^3)$.

(F) $\mathbb{Z}[t]/\langle 2t, t^2-2\rangle$.
b) We have $u(\mathbb{Z}[t]/\langle 2t, t^2-2\rangle) = -1$.

The argument that a finite local ring with cyclic unit group must be isomorphic to one of the rings listed in Theorem 5.14a) is rather intricate, and we refer the interested reader to Gilmer's paper [Gi63]. We will now prove the rest of Theorem 5.14.

Proof. a) First we check that the rings (A) through (F) have cyclic unit group. For (A) this is Corollary 5.6. For (B) and (C) this is Theorem 4.1. For (E), this is Example 3.2c).

As for (D): the ring $R = \mathbb{Z}/p\mathbb{Z}[t]/(t^2)$ is a finite local of order p^2 with maximal ideal $\langle t\rangle$ of order p, so the unit group $U(R)$ has order $p(p-1)$. Because $U(p) \subset U(R)$, by part (A) the group $U(R)$ has an element of order $p-1$. The group $U(R)$ has an element of order p: this special case of Cauchy's Theorem follows from Theorem 5.1a). Since $\gcd(p-1,p)$, the subgroup generated by these two elements is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}/(p(p-1))$.

As for (F): put $T = \mathbb{Z}[t]/\langle 2t, t^2-2\rangle$. In T we have

$$4 = 2 \cdot 2 = 2t^2 = t(2t) = 0.$$

Therefore T is the quotient of the ring $\mathbb{Z}/4\mathbb{Z}[x]/(x^2-2)$, which has 16 elements, by the ideal generated by $2t$, which has two elements, so T has eight elements, represented by $0, 1, 2, 3, t, t+1, t+2, t+3$. We claim that the unit group is cyclic of order 4, generated by $t+1$. First of all, we have

$$t+1,\ 3 = (t+1)^2,\ t+3 = (t+1)^3, 1 = (t+1)^4,$$

so $t+1 \in U(T)$ has order 4. For every other $x \in T$, $x^3 = 0$, so $U(T)$ is cyclic, generated by $t+1$. The element t is not a unit, so the principal ideal $\mathfrak{m} = \langle t\rangle$ is proper. The ideal $\mathfrak{m}$ contains $0 = 0 \cdot t$, $2 = t \cdot t$, $t = 1 \cdot t$ and $t+2 = (t+1) \cdot t$, so $\mathfrak{m} = T \setminus U(T)$. It follows that $\mathfrak{m}$ is the unique maximal ideal, so T is a local ring. For later reference we mention that T is a principal ring, i.e., every ideal is principal. Indeed, in a local ring of order 8, a nonzero nonmaximal ideal must have order 2 and thus is certainly principal.[3] Finally, we have

$$u(T) = 1 \cdot 3 \cdot (t+1) \cdot (t+3) = 3(t^2+4t+3) = -(t^2-1) = -(2-1) = -1. \qquad \square$$

Putting these results together we get the result of Hirano-Matsuoka.

Theorem 5.15 (Wilson's Theorem in a Finite Ring [HM13])**.**
Let R be a finite ring. Suppose that $R \cong \prod_{i=1}^r R_i$ is a product of local rings. Then:
a) If the number of i for which R_i is not *a finite field of even order is either 0 or is at least 2, then $u(R) = 1$.*
b) Otherwise there is exactly one i for which R_i is not a finite field of even order, and $u(R) = (1, \ldots, 1, u(R_i), 1, \ldots, 1)$. More precisely:
(i) If R_i has odd order, then $u(R_i) = -1$.
(ii) If R_i is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or to $\mathbb{Z}[t]/\langle 2t, t^2-2\rangle$ then $u(R_i) = -1$.
(iii) If R_i is isomorphic to $\mathbb{Z}/2\mathbb{Z}[t]/(t^2)$ then $u(R_i) = t+1$.
(iv) If R_i is isomorphic to $\mathbb{Z}/2\mathbb{Z}[t]/(t^3)$ then $u(R_i) = t^2+1$.
(v) Otherwise $u(R) = u(R_i) = 1$.

6. The Product of the Zero-Divisors in a Finite Ring

In elementary number theory courses, Wilson's Theorem is often supplemented by the remark that primes are characterized as precisely the integers $n \geq 2$ satisfying the congruence $(n-1)! \equiv -1 \pmod{n}$. Indeed, for $n \in \mathbb{Z}^+$, put

$$T_n \coloneqq \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\bullet} x \in \mathbb{Z}/n\mathbb{Z}.$$

[3] In fact in any Noetherian local ring with principal maximal ideal is a principal ring, i.e., every ideal is principal [**?**, Prop. 16.5].

When n is prime we have $T_n = S_n = -1$. But when n is composite there is some $1 < d < n$ which divides n, and thus T_n is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$, whereas -1 is a unit in $\mathbb{Z}/n\mathbb{Z}$, so certainly $T_n \neq -1$. However we can say more.

Proposition 6.1. *a) If n is prime, then $T_n = S_n = -1$.*
b) We have $T_4 = 2$.
c) If $n \geq 6$ is composite, then $T_n = 0$.

Proof. a) This is Wilson's Theorem. b) We have $(4-1)! \equiv 2 \pmod 4$.
c) First suppose $n = p^2$ for an (odd, since $n > 4$) prime p. Then $2p < p^2$, so

$$p^2 \mid p \cdot 2p \mid (p^2 - 1)!$$

If $n \geq 6$ is composite and not of the form p^2, then let p be the smallest prime divisor of n. Then $1 < p < \frac{n}{p} < n$, so

$$n = p(\frac{n}{p}) \mid (n-1)!. \qquad \square$$

Proposition 6.1 seems less interesting than Gauss's Theorem 4.1. For composite n, taking the product over all units modulo n seems to be a closer analogue of $(p-1)!$ when p is prime than $(n-1)! \pmod n$ is. It would be silly to ask for the value of $n!$ modulo n: clearly it is 0. When n is composite, asking for $(n-1)!$ modulo n is almost as silly: the product includes all proper zero divisors in $\mathbb{Z}/n\mathbb{Z}$. In a ring with proper zero divisors, if we multiply all of them together, surely the most likely outcome is 0.

But there was one outlying case: in $\mathbb{Z}/4\mathbb{Z}$, 2 is the unique proper zero divisor, so the product over all the zero divisors (and thus all the elements) is not 0. We wonder: is there any other finite ring, not an integral domain, such that the product over all proper zero divisors is nonzero? In fact yes:

Example 6.2. *In $R = \mathbb{Z}/2\mathbb{Z}[t]/(t^2)$, we have*

$$\prod_{x \in R^\bullet} x = 1 \cdot t \cdot (t+1) = t^2 + t = t.$$

We will find all finite rings R such that $\prod_{x \in R^\bullet} x \neq 0$. In fact we can set things up so as to treat infinite rings as well.

Lemma 6.3. *Let p be a prime number.*
a) Every ring of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.
b) Every ring of order p^2 is isomorphic to exactly one of the following rings: $\mathbb{Z}/p^2\mathbb{Z}$; "the" finite field $\mathbb{F}_{p^2}$; $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$; or $\mathbb{Z}/p\mathbb{Z}[t]/(t^2)$.

Proof. a) The subring generated by 1 must be all of R.
b) The subring generated by 1 is either all of R – in which case $R \cong \mathbb{Z}/p^2\mathbb{Z}$ – or it is $\mathbb{Z}/p\mathbb{Z}$. In the latter case, let $T \in R \setminus \mathbb{Z}/p\mathbb{Z}$; then there is a unique homomorphism $\varphi : \mathbb{Z}/p\mathbb{Z}[t] \to R$ sending $t \mapsto T$; since its image in a ring of order p^2 properly contains a subring of order p, this map is surjective. Since $\mathbb{Z}/p\mathbb{Z}[t]$ is a principal ideal domain, the kernel of φ is generated by a single monic polynomial, which order considerations show must have degree 2: thus there are $b, c \in \mathbb{Z}/p\mathbb{Z}$ such that

$$\mathbb{Z}/p\mathbb{Z}[t]/(t^2 + bt + c) \cong R.$$

If the polynomial $t^2 + bt + c$ is irreducible, R is a field. If $t^2 + bt + c = (t+r)(t+s)$ for $r \neq s$, then by the Chinese Remainder Theorem we have

$$R \cong \mathbb{Z}/p\mathbb{Z}[t]/(t+r)(t+s) \cong \mathbb{Z}/p\mathbb{Z}[t]/(t+r) \cong \mathbb{Z}/p\mathbb{Z}[t]/(t+s) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Finally, if $t^2 + bt + c = (t+r)^2$, then

$$R \cong \mathbb{Z}/p\mathbb{Z}[t]/(t+r)^2 \cong \mathbb{Z}/p\mathbb{Z}[t]/(t^2);$$

the last isomorphism is obtained by mapping $t \mapsto t - r$. $\square$

Theorem 6.4. *Let R be a nonzero ring that is* not *an integral domain. The following are equivalent:*
(i) For all distinct $x, y \in R^\bullet$*, we have $xy \neq 0$.*
(ii) R is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or to $\mathbb{Z}/2\mathbb{Z}[t]/(t^2)$.
(iii) R is finite, contains a unique proper zero divisor t, and $\prod_{x \in R^\bullet} x = t$.

Proof. (i) $\implies$ (ii): **Step 1**: We show that R has at most 4 elements. Since R is not an integral domain, it has a proper zero divisor x. Since for all $y \notin \{0, x\}$ we have $xy \neq 0$, it must be the case that $x^2 = 0$. Consider now the map $\cdot x : R \to R$ given by $y \mapsto xy$. This is a homomorphism from the additive group $(R, +)$ to itself; let K be its kernel and I its image, so $R/K \cong I$. If R has more than 4 elements, then either K or I has at least 3 elements (otherwise R is the union of at most two cosets of a subgroup of order at most two). If K has at least 3 elements, it has an element $y \notin \{0, x\}$ and thus x, y are distinct nonzero elements with $xy = 0$: contradiction. If I has at least 3 elements, then I has an element $y = xz \notin \{0 = 0x, x = 1x\}$. Then x, y are distinct nonzero elements with $xy = x(xz) = x^2 z = 0z = 0$: contradiction.
Step 2: By Lemma 6.3 the only nonzero rings of order at most 4 that are not integral domains are $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}[t]/(t^2)$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have $(1, 0) \cdot (0, 1) = (0, 0) = 0$.
(ii) $\implies$ (iii): This was shown above.
(iii) $\implies$ (i): For distinct $x, y \in R^\bullet$, at least one is not a zero divisor, so $xy \neq 0$. □

7. Wilson Semi-Products

In this final section we discuss a topic that connects algebra to classical number theory in a different way: via algebraic number theory. We will not emerge with a definitive result, but we point out some opportunities for further work.

Let R be a nonzero finite commutative ring of odd order. Then its unit group $U(R)$ has even order: by Theorem 5.8 and (1) we reduce to the case in which R has a unique maximal ideal $\mathfrak{m}$, and then since $\#\mathfrak{m}$ divides $\#R$ we have that $\#\mathfrak{m}$ is odd, hence $\#U(R) = \#R - \#\mathfrak{m}$ is even. It follows from Lemma 5.7 that $\{\pm 1\}$ is a subgroup of the unit group $U(R)$. A **semi-system** on R is a subset H of $U(R)$ such that for all $u \in U(R)$, exactly one of $\pm u$ lies in H; equivalently, it is a set of coset representatives of $\{\pm 1\}$ in $U(R)$. The number of semi-systems is thus $2^{\#\frac{U(R)}{2}}$.

Example 7.1. *If $R = \mathbb{Z}/p\mathbb{Z}$, then $H_\bullet := \{1, \ldots, \frac{p-1}{2}\}$ is a semi-system.*

For a semi-system H on a finite commutative ring R of odd order, we define the **Wilson semi-product**

$$u_H(R) := \prod_{x \in H} x.$$

The element $u_H(R)$ depends on the choice of H, but in an understandable way: if H_0 is any semi-system, then for exactly half of the semi-systems H we have $u_H(R) = u_{H_0}(R)$, and for the other half we have $u_H(R) = -u_{H_0}(R)$. One can see this for instance by defining an involution $H \mapsto \overline{H}$ on semi-systems by replacing 1 by -1 if 1 lies in H and replacing -1 by 1 if -1 lies in H.

Proposition 7.2.
Let R be a nonzero finite commutative ring of odd order, and let $H \subset R^\times$ be a semi-system.
a) If R is local and $\#R^\times \equiv 2 \pmod 4$, then we have $u_H(R) \in \{\pm 1\}$.
b) If R is local and $\#R^\times \equiv 0 \pmod 4$, then $u_H(R)$ has order 4 in $R^\times$.
c) If R is not local, then $u_H(R)^2 = 1$.

Proof. Put $s := \#H = \frac{\#R^\times}{2}$. Then

$$u(R) = \prod_{x \in U(R)} x = \prod_{x \in H} x \prod_{x \in U(R) \setminus H} x = (-1)^s u_H(R)^2. \tag{4}$$

By Theorem 5.11 we have $u(R) = -1$ if R is local and $u(R) = 1$ otherwise. Thus if R is local and $\#R^\times \equiv 0 \pmod 4$ then $u_H(R)^2 = -1$, so $u_H(R)$ has order 4, whereas in all other cases we have

$u_H(R)^2 = 1$. As we have seen, in a general ring $x^2 = 1$ need not imply $x \in \{\pm 1\}$, but the proof of Theorem 5.11a) shows that this implication does hold when R is local of odd order. □

Proposition 7.2 evaluates the Wilson semi-products when $R = \mathbb{F}_q$ is a finite field of odd order: if $q \equiv 1 \pmod 4$, then $u_H(\mathbb{F}_q)$ has order 4. Since $U(\mathbb{F}_q)$ is cyclic, there are two elements of order 4, and as above both are possible. If $q \equiv 3 \pmod 4$ then $u_H(\mathbb{F}_q) \in \{\pm 1\}$, and again both are possible.

But not so fast! This time our abstract perspective has actually obscured the most interesting part. Let's reconsider the simplest case of $R = \mathbb{Z}/p\mathbb{Z}$ for an odd prime p. If $p \equiv 3 \pmod 4$, then for half of the semi-systems H we have $u_H(\mathbb{Z}/p\mathbb{Z}) = 1$ and for half we have $u_H(\mathbb{Z}/p\mathbb{Z}) = -1$. In Example 7.1 we singled out a semi-system $H_\bullet = \{1, \ldots, \frac{p-1}{2}\}$. Then we have

$$u_{H_\bullet}(\mathbb{Z}/p\mathbb{Z}) = \frac{p-1}{2}! \pmod p \in \{\pm 1\}.$$

Well, which is it?? The answer lies much deeper:

Theorem 7.3 (Mordell [Mo61]). *Let $p > 3$ be a prime number with $p \equiv 3 \pmod 4$. Then $u_{H_\bullet}(\mathbb{Z}/p\mathbb{Z}) = 1$ iff the class number $h(-p)$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ is congruent to 3 modulo 4.*

For a squarefree integer $n \equiv 1 \pmod 4$, the class number $h(n)$ of the quadratic field $\mathbb{Q}(\sqrt{n})$ is the number of equivalence classes of nonzero ideals in the ring $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ under the relation $I \sim J$ iff there are nonzero $\alpha, \beta \in \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ such that $\alpha I = \beta J$. Unfortunately this definition is not immediately enlightening. The class number of a number field is a central topic of study in the field of algebraic number theory, the roots of which are both old and deep. Indeed, Mordell deduces Theorem 7.3 from several results of Dirichlet, including his analytic class number formula.

Though it is not obvious from the definition, already by 1800 it was known that for a prime $p \equiv 3 \pmod 4$, the class number $h(-p)$ is odd. (Early number theorists used an equivalent definition of $h(-p)$ in terms of classes of binary quadratic forms.) There is no correspondingly simple criterion for class numbers modulo 4. There ought to be infinitely many primes $p \equiv 3 \pmod 4$ such that $h(-p) \equiv 1 \pmod 4$ and infinitely many with $h(-p) \equiv 3 \pmod 4$, but I believe that both are open questions.

Now let $p \equiv 1 \pmod 4$, so $u_{H_\bullet}(\mathbb{Z}/p\mathbb{Z}) = \frac{p-1}{2}! \pmod p$ is one of the two fourth roots of unity in $\mathbb{Z}/p\mathbb{Z}$. Which one? Chowla [Ch61] answers this question in terms of the arithmetic of the ring of integers $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ of the real quadratic field $\mathbb{Q}(\sqrt{p})$, which we view as a subfield of $\mathbb{R}$. Also in this case the class number $h(p)$ is odd, and we have

$$U(\mathbb{Z}[\frac{1+\sqrt{p}}{2}]) = \{\pm 1\} \times U^+$$

with U^+ the subgroup of positive units. Then U^+ is infinite cyclic; let

$$\epsilon_p := \frac{u_p + \sqrt{p} v_p}{2}$$

be the generator of U^+ that is greater than 1, the "fundamental unit" of $\mathbb{Q}(\sqrt{p})$.

Theorem 7.4 (Chowla [Ch61]). *For a prime number $p \equiv 1 \pmod 4$, we have*

$$\frac{p-1}{2}! \equiv \frac{1}{2}(-1)^{\frac{h(p)+1}{2}} u_p \pmod p.$$

Since ϵ_p is a unit, we have $u_p^2 + p v_p^2 = \pm 4$. Using this we see that

$$\left(\frac{p-1}{2}!\right)^2 \equiv \left(\frac{1}{2}(-1)^{\frac{h(p)+1}{2}} u_p\right)^2 \equiv \pm 1 \pmod p.$$

By Proposition 7.2 we know that $\frac{p-1}{2}! \pmod p$ has order 4, so we deduce that

$$u_p + p v_p^2 = -4,$$

i.e., fundamental unit of $\mathbb{Q}(\sqrt{p})$ has norm -1. This is a nontrivial number-theoretic result.

For any odd $n \in \mathbb{Z}^+$ there is a canonical semi-system in $\mathbb{Z}/n\mathbb{Z}$, namely

$$H_\bullet := \{1 \leq k \leq \frac{n-1}{2} \mid \gcd(k,n) = 1\}.$$

These Wilson semi-products were studied by Cosgrave and Dilcher [CD08] .[4] For all odd n they compute [CD08, Thm. 2] the order of $u_{H_\bullet}(\mathbb{Z}/n\mathbb{Z})$ in $U(n)$, and they explicitly determine $u_{H_\bullet}(\mathbb{Z}/n\mathbb{Z})$ in certain cases. From our perspective, when the order is 2, one would also like to know when it is -1: if not, then $u_H(\mathbb{Z}/n\mathbb{Z})$ has order 2 for all H, and if so, then $u_H(\mathbb{Z}/n\mathbb{Z}) = 1$ for some H. E.g. it follows from their general results that $u_{H_0}(\mathbb{Z}/15\mathbb{Z})$ has order 2. In fact $u_{H_0}(\mathbb{Z}/15\mathbb{Z}) = 11 \in \mathbb{Z}/15\mathbb{Z}$, so as H ranges over all semi-systems, the values of $u_H(\mathbb{Z}/15\mathbb{Z})$ are 4 and 11.

A recent paper of Li-Sha [LS17] gives analogues of the results of Mordell and Cosgrave-Dilcher for rings of the form $\mathbb{F}_q[t]/(n(t))$ for an odd prime power q. We will restrict our attention to one interesting case: Let $p \equiv 3 \pmod 4$ be a prime number and $P \in \mathbb{Z}/p\mathbb{Z}[t]$ be irreducible of odd degree d, so that $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}[t]/(P)$ is a finite field of order $p^d \equiv 3 \pmod 4$. For any semisystem H in $\mathbb{F}$, Proposition 7.2 gives that $u_H \in \{\pm 1\}$. Starting from any semisystem $\mathfrak{s}$ in $\mathbb{Z}/p\mathbb{Z}$, one obtains a semisystem in $\mathbb{F}$ by taking the polynomials of degree less than d with leading coefficient in $\mathfrak{s}$. We will choose the semisystem H_P obtained in this way from $\mathfrak{s} = \{1, \ldots, \frac{p-1}{2}\}$. Let $h(-P)$ be the class number of the function field $\mathbb{F}_q(t, \sqrt{-P(t)})$. This can be described concretely as nonzero ideals modulo nonzero principal ideals as above, but in the ring $\mathbb{F}_p[x,y]/(y^2 + P(x))$.[5] Then we get the following result, an equivalent formulation of a special case of [LS17, Thm. 4.1].

Theorem 7.5. a) *If $h(-p) \equiv h(-P) \pmod 4$, then $u_{H_P} = -1$.*
b) *If $h(-p) \not\equiv h(-P) \pmod 4$, then $u_{H_P} = 1$.*

In [W67], Weil wrote: "[I]t goes without saying that the function-fields over finite fields must be granted a fully simultaneous treatment with number-fields, instead of the segregated status, and at best the separate but equal facilities, which hitherto have been their lot." By this he meant, I think, that one should pursue results for number fields and function fields at the same time. But I am not sure that I have ever seen the two sitting down at the table of brotherhood quite like this.

In the case when the irreducible polynomial $P \in \mathbb{Z}/p\mathbb{Z}[t]$ has even degree, the results of Li-Sha tell us that for any semisystem H in $\mathbb{Z}/p\mathbb{Z}[t]/(P)$, the order of u_H is 4...as we already knew. In this case, if the leading coefficient of $-P$ is a square, then $\mathbb{Z}/p\mathbb{Z}(t, \sqrt{-P})$ is a "real quadratic function field," so one should seek an analogue of Chowla's result [Ch61] giving the answer in terms of a generator of the infinite cyclic group $U(\mathbb{Z}/p\mathbb{Z}[x,y]/(y^2 + P(x)))/U(\mathbb{Z}/p\mathbb{Z})$.

It would also be interesting to find further semi-systems in finite commutative rings for which the evaluation of a Wilson semi-product comes out in terms of a class number or better still to find a more general algebraic framework that explains the appearance of class numbers.

8. Complements

8.1. **The Vandiver-Weaver Theorem.** The following result of Vandiver-Weaver [VW58, Thm. 4.4.9] is a generalization of Theorem 1.4.

Theorem 8.1.
Let G be a finite commutative group of order $2n$, and let a be an element of G. The map $\iota_a : G \to G$ given by $x \mapsto ax^{-1}$ is an involution on G: $\iota_a^2 = 1_G$. Let f be the number of fixed points of ι_a, and let t be any order 2 element of G. Then $\prod_{x \in G} x = a^n t^{\frac{f}{2}}$.

[4] More generally, for $N, n \in \mathbb{Z}^+$, they consider the **Gauss factorial** $N_n! := \prod_{1 \leq k \leq N,\ \gcd(k,n)=1} k \in U(n)$.

[5] Beware that we need d to be odd for this description of the class group to be valid.

Proof. Step 1: The same calculation as in §1.4 shows that ι_a is an involution. Suppose first that there is no $x \in G$ such that $x^2 = a$. Then ι_a is fixed point free and the same argument as in §1.4 shows that $\prod_{x \in G} x = a^n = a^n t^{\frac{0}{2}}$, establishing the result in this case.
Step 2: Suppose there is $A \in G$ be such that $A^2 = a$. The map $x \mapsto Ax$ gives a bijection from $G[2]$ to the set $F = \{x \in G \mid x^2 = a\}$ of fixed points of ι_a: if $x^2 = e$, then $(Ax)^2 = A^2x^2 = a$, and if $x \in F$ then $(\frac{x}{A})^2 = \frac{x^2}{A^2} = e$. Let $f = \#F = \#G[2]$. Since $\#G$ and $\#(G \setminus F)$ are even, so is f. By Theorem 1.4, if $f = 2$ then $\prod_{y \in G[2]} y = t = t^{\frac{f}{2}}$, while if $f \geq 4$ then $\prod_{y \in G[2]} y = e = t^{\frac{f}{2}}$.
Step 3: The elements of $G \setminus F$ consist of $n - \frac{f}{2}$ pairs of distinct $x, y \in G$ such that $xy = a$, so

$$\prod_{x \in G} x = \prod_{x \in G \setminus F} x \prod_{x \in F} x = a^{n - \frac{f}{2}} \prod_{y \in G[2]} Ay = a^{n - \frac{f}{2}} A^f \prod_{y \in G[2]} y = a^n t^{\frac{f}{2}}. \qquad \square$$

It would be interesting to have an application that uses Theorem 8.1 and not just Theorem 1.4.

8.2. **Remarks on the history and the literature.**

Wilson's Theorem is named after the British mathematician John Wilson (1741-1793). As for many other results in the subject, this attribution seems faulty. Wilson *conjectured* the result while a student at Cambridge. He conveyed it to Edward Waring, the Lucasian Chair of Mathematics, who announced it as a conjecture in 1770. Leibniz had also conjectured it in the 17th century, although he did not publish it. In fact the statement appears in the work of the Arabic polymath Ibn al-Haytham circa 1000 [Ra80]. It was first proved by Lagrange in 1771.

Gauss's generalization of Wilson's Theorem appears in [G, Art. 78].

So far as I know, Theorem 1.4 was first proved by the early American group theorist George Abram Miller (1863-1951) [Mi03]. It has been rediscovered and published several times: e.g. [Oh77, Lemma 1], [D09, Lemma 4], but I have not been able to find it in any standard textbook.

The proof of Theorem 1.4 given in §1.3 seems to be new. The proof given in §1.4 is very similar to that of Saucier [Sa18, p. 100]. It is also similar to an argument of Górowski-Łomnicki [GL14]. In [GL14] the involution ι_a is not quite made explicit but its essential use is eventually revealed: "By Lemma 2.2 the elements of $G[2] \setminus \{1, a\}$ can be arranged in pairs (x, y) such that $xy = a$ and $x \neq y$." It seems to me that building the proof around the involution ι_a shortens and simplifies it. Saucier also gives a proof in which the involution ι_a features implicitly and is understood and constructed via an interesting counting argument. Of course the notion of an involution ι_a goes back to Vandiver-Weaver [VW58]. I must confess however that I find the exposition of [VW58, §4.4] to be somewhat opaque.

Following [Sa18], we supply some motivation for the second proof in hindsight. To give a fixed point free involution on a set X is equivalent to giving a partition of X into 2 element subsets. If G is a commutative group in which every nonidentity element has order 2 and a is a nonidentity element of G, then the partition of G associated to the involution ι_a is the partition into cosets of the subgroup $\{1, a\}$. Thus the two proofs are "dual" in the sense that we may view G as a $\mathbb{Z}/2\mathbb{Z}$-vector space, and whereas the first proof sums over cosets of a codimension one subspace, the second proof sums over cosets of a one-dimensional subspace. We leave for the reader to decide which of the two proofs is more suitable for classroom presentation. In my opinion the second proof is shorter and faster to follow line-by-line but may be more slick than transparent. On the other hand there is some precedent for using well-chosen involutions to give short, snappy proofs of results in number theory: see e.g. [Za90].

The main tools Gilmer uses to prove Theorem 5.14a) are Theorems 5.8 and 4.1. Several other proofs have been given, some extending the result to infinite rings [Ay69], [EF67], [PS70]. Theorem 5.15 in the case of a residue ring $\mathbb{Z}_K/\mathfrak{n}$ of the ring of integers of a quadratic number field K is due to Ohnari

[Oh77]. For an arbitrary number field K it was proved by Lassak [La00] and then, more simply, by Dalawat [D09]. By [BC15, Thm. 1.12] this case coincides (up to isomorphism) with the class of all finite principal rings.[6] That fifty years elapsed between [Gi63] and [HM13] seems strange, but better late than never. Our proof of Theorem 5.15 is different from Hirano-Matsuoka's and perhaps more broadly accessible: it leans more heavily on group theory than ring theory.

Theorem 6.4 appears to be new, but it is a consequence of two older results. For a ring R, Anderson-Livingston [AL99] define a graph $\Gamma(R)$ with vertices the proper zero divisors of R and in which x, y are connected by an edge iff $x \neq y$ and $xy = 0$. Thus R satisfies condition (i) of Theorem 6.4 iff $\Gamma(R)$ has no edges. Anderson-Livingston show – in any ring – that any two vertices in $\Gamma(R)$ are connected by a path of length at most 3. So $\Gamma(R)$ can only have no edges if there is only one vertex, i.e., there is a unique proper zero divisor. Next there is a result of Ganesan [Ga64]: if a ring R has exactly $n \geq 2$ zero divisors, then R has order at most n^2. So a ring with a unique proper zero divisor has size at most 4. The proof of Ganesan's Theorem is similar to the argument we gave: if x is a proper zero divisor, the kernel K of multiplication by x consists of zero divisors so has size at most n, and there is an injective homomorphism $(R/K, +) \stackrel{\cdot x}{\to} (R, +)$, whose image consists of zero divisors, so R has at most n^2 elements.

8.3. **Other proofs of Wilson's Theorem.**

Our proof of Wilson's Theorem is a standard one, and it is essentially Lagrange's proof. Let us quickly run through a few other proofs: throughout p is an odd prime.

• (Gerrish [Ge72]) In the symmetric group S_p, the Sylow p-subgroups are cyclic of order p. The order p elements of S_p are precisely the p-cycles, of which there are $p!/p = (p-1)!$. Since a cyclic group of order p has $p-1$ generators, the number of Sylow p-subgroups is $n_p = (p-1)!/(p-1) = (p-2)!$ According to the Sylow Theorems, we have $n_p \equiv 1 \pmod{p}$, i.e., $(p-2)! \equiv 1 \pmod{p}$ and thus

$$(p-1)! \equiv (p-1)(p-2)! \equiv -1 \pmod{p}.$$

• Lagrange's Theorem and the Root-Factor Theorem yield the polynomial identity

$$t^{p-1} - 1 = (t-1)(t-2)\cdots(t-(p-1)) \in \mathbb{Z}/p\mathbb{Z}[t].$$

Evaluating at 0 gives

$$-1 \equiv (-1)^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

• If we can establish that $U(p)$ is cyclic, we can apply Example 1.1. By Corollary 5.6, the unit group of a finite field is cyclic. However, this deduction used the Structure Theorem for Finite Commutative Groups. We can avoid this as follows.

Theorem 8.2 (Cyclicity Criterion)**.** *Let G be a (not necessarily commutative) finite group. If for all $d \in \mathbb{Z}^+$ we have $\#\{x \in G \mid x^d = e\} \leq d$, then G is cyclic.*

Proof. **Step 1:** For $n \in \mathbb{Z}^+$, let $\varphi(n)$ be the order of $U(n)$. Observe that $\varphi(n)$ is also the number of generators of the cyclic group $(\mathbb{Z}/n\mathbb{Z}, +)$. Every $1 \leq k \leq n$ generates a cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z}, +)$, and for each $d \mid n$ there is a unique order d cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z}, +)$. Therefore $n = \sum_{d|n} \varphi(d)$.
Step 2: Suppose G has order n. For $d \in \mathbb{Z}^+$, let $f(d)$ be the number of elements of G of order d. By Lagrange's Theorem $f(d) = 0$ unless $d \mid n$, so $n = \sum_{d|n} f(d)$. If $d \mid n$ and $f(d) \geq 1$ then G has a cyclic subgroup C_d of order d. We have $x^d = e$ for all $x \in C_d$, so by hypothesis C_d contains all such elements of G and thus all elements of order d. Therefore $f(d) = 0$ or $f(d) = \varphi(d)$, so $f(d) \leq \varphi(d)$. So

$$n = \sum_{d|n} f(d) \leq \sum_{d|n} \varphi(d) = n,$$

[6] It follows from Theorem 5.14 that if R is a finite ring with cyclic unit group then it is a principal ring. It would be interesting to establish this directly and thus reduce Gilmer's Theorem to the Lassak-Dalawat Theorem.

so $f(d) = \varphi(d)$ for all $d \mid n$. In particular $f(n) = \varphi(n) \geq 1$, so G is cyclic. □

We can use Theorem 8.2 in place of Theorem 5.2 in the proof of Corollary 5.6, getting a more elementary proof that the unit group of a finite field is cyclic.

The last two proofs immediately adapt to show $u(F) = -1$ for any finite field F, but Gerrish's proof does not. This is a feature it shares with several combinatorial proofs of Wilson's Theorem, some of which solve a more general counting problem parameterized by a positive integer n which reduces to Wilson's Theorem when n is prime [Gu85], [An11], [Tr18]. It also shares this feature with the proofs that use group actions on finite sets [F58], [EH05]. It is tempting to see how many of the combinatorial proofs of Wilson's Theorem can be "algebraicized" by recasting them in terms of group actions, but we will leave this exploration to the interested reader.

References

[An11] S.A. András, *A combinatorial generalization of Wilson's theorem.* Australas. J. Combin. 49 (2011), 265–272.

[AL99] D.F. Anderson and P.S. Livingston, *The zero divisor graph of a commutative ring.* J. Algebra 217 (1999), 434–447.

[Ay69] C.W. Ayoub, *On finite primary rings and their groups of units.* Compositio Math. 21 (1969), 247–252.

[BC15] A. Brunyate and P.L. Clark, *Extending the Zolotarev-Frobenius approach to quadratic reciprocity.* Ramanujan J. 37 (2015), 25–50.

[C-CA] P.L. Clark, *Commutative Algebra.* `http://math.uga.edu/~pete/integral.pdf`

[C-NT] P.L. Clark, *Number Theory: A Contemporary Introduction.* `http://math.uga.edu/~pete/4400FULL.pdf`

[Ch61] S. Chowla, *On the class number of real quadratic fields.* Proc. Nat. Acad. Sci. USA 47 (1961), 878.

[CD08] J.B. Cosgrave and K. Dilcher, *Extensions of the Gauss-Wilson theorem.* Integers 8 (2008), A39, 15 pp.

[D09] C.S. Dalawat, *Wilson's theorem.* J. Théor. Nombres Bordeaux 21 (2009), 517–521.

[EF67] K.E. Eldridge and I. Fischer, *D.C.C. rings with a cyclic group of units.* Duke Math. J. 34 (1967), 243–248.

[EH05] T.J. Evans and B.V. Holt, *Deriving divisibility theorems with Burnside's theorem.* Integers 5 (2005), no. 1, A26, 5 pp.

[F58] W. Feit, *Classroom Notes: A Group-Theoretic Proof of Wilson's Theorem.* Amer. Math. Monthly 65 (1958), 120.

[G] K.F. Gauss, *Disquisitiones Arithmeticae.* Springer-Verlag, New York, 1986.

[Ga64] N. Ganesan, *Properties of rings with a finite number of zero divisors.* Math. Ann. 157 (1964), 215–218.

[Ge72] F. Gerrish, *Sledge-hammer cracks peanut.* Math. Gaz. 56 (1972), 38–39.

[Gi63] R.W. Gilmer Jr., *Finite rings having a cyclic multiplicative group of units.* Amer. J. Math. 85 (1963), 447–452.

[GL14] J. Górowski and Łomnicki, *Simple proofs of some generalizations of the Wilson's theorem.* Ann. Univ. Paedagog. Crac. Stud. Math. 13 (2014), 7–14.

[Gu85] H. Gupta, *A theorem in combinatorics and Wilson's theorem.* Amer. Math. Monthly 92 (1985), 575–576.

[HM13] Y. Hirano and M. Matsuoka, *Finite rings and Wilson's theorem.* Turkish J. Math. 37 (2013), 571–576.

[La00] M. Lassak, *Wilson's theorem in algebraic number fields.* Math. Slovaca 50 (2000), 303–314.

[LS17] X. Li and M. Sha, *Gauss factorials of polynomials over finite fields.* Int. J. Number Theory 13 (2017), 2039–2054.

[Mi03] G.A. Miller, *A new proof of the generalized Wilson's theorem.* Ann. of Math. (2) 4 (1903), 188–190.

[Mo61] L. J. Mordell, *The congruence* $\frac{p-1}{2}! \equiv \pm 1 \pmod{p}$. Amer. Math. Monthly 68 (1961), 145–146.

[Oh77] S. Ohnari, *On the extension of Wilson's theorem to quadratic fields.* Hitotsubashi J. Arts Sci. 18 (1977), 55–67.

[PS70] K.R. Pearson and J.E. Schneider, *Rings with a cyclic group of units.* J. Algebra 16 (1970), 243–251.

[Ra80] R. Rashed, *Ibn al-Haytham et le théorème de Wilson.* Arch. Hist. Exact Sci. 22 (1980), 305–321.

[R] M. Rosen, *Number theory in function fields.* Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002.

[Sa18] C. Saucier, *A combinatorial approach to Wilson's theorem for finite Abelian groups.* Math. Mag. 91 (2018), 97–102.

[SG85] J.L. Smith and J.A. Gallian, *Factoring finite factor rings.* Math. Mag. 58 (1985), 93–95.

[Tr18] E. Treviño, *An inclusion-exclusion proof of Wilson's theorem.* College Math. J. 49 (2018), 367–368.

[VW58] H.S. Vandiver and M.W. Weaver, *Introduction to arithmetic factorization and congruences from the standpoint of abstract algebra.* Amer. Math. Monthly 65 1958 no. 8, part II, 53 pp.

[W67] A. Weil, *Basic number theory.* Die Grundlehren der mathematischen Wissenschaften, Band 144 Springer-Verlag New York, Inc., New York 1967.

[Za90] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod{4}$ *is a sum of two squares.* Amer. Math. Monthly 97 (1990), 144.