WILSON'S THEOREM: AN ALGEBRAIC APPROACH

PETE L. CLARK

Abstract. We discuss three algebraic generalizations of Wilson's Theorem on congruences: 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 primes p, $(p-1)! \equiv -1 \pmod{p}$ – to the widest possible mathematical audience.

The standard proof of Wilson's Theorem proceeds by evaluating the product of all elements in the unit group $U(p)$ 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 and prove such a result, a theorem of G.A. Miller. Our proof should be accessible to those studying group theory for the first time. In §2 we consider the case of $U(n)$, the unit group of the finite 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 – which has a close analogy to the case of $\mathbb{Z}/n\mathbb{Z}$ – 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 comment on the history, the literature and other proofs of Wilson's Theorem.

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 $(R, +)$. The unit group of a ring R – i.e., the multiplicative group of $x \in R$ for which there is $y \in R$ with $xy = 1$ – will be denoted $U(n)$. We write $R^\bullet$ for $R \setminus \{0\}$. 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 ring without proper zero divisors.

1. Wilson's Theorem in a Finite Commutative Group

Let $(G, \cdot)$ be a finite commutative group, with identity element e. Let $S = \prod_{x \in G} x$ be the product of all elements of G. Can we determine S?

Example 1.1. *Suppose G is cyclic of order n. We identify G with the additive group $(\mathbb{Z}/n\mathbb{Z}, +)$ of integers modulo n. Then*

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

- *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 $x = \pm 1$. (Since p is odd, 1 and -1 are distinct elements of $U(p)$.) For every element $x \in U(p)$ with $x^2 \neq 1$, 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, $(p-1)! \equiv -1 \pmod{p}$.*

We return to the general case. As in Example 2, 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: if $x = x^{-1}$ and $y = y^{-1}$ then $(xy)^{-1}) = y^{-1}x^{-1} = yx = xy$. Thus we reduce the general case to the case $G = G[2]$.

Lemma 1.4. *Suppose every element of G has order at most two. 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. An easy exercise left to the reader. □

Lemma 1.5. *Suppose every element of G has order at most two.*
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 1.4 $H_1 = \{e, x_1\}$ is a subgroup of order 2. If $G = H_1$, we're done. Otherwise there is $x_2 \in G \setminus H_1$, and applying Lemma 1.4 again 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 obtain a sequence of subgroups

$$\{e\} = H_0 \subset H_1 \subset \ldots \subset H_n \subset \ldots;$$

H_n has order 2^n. Since G is finite we must have $H_k = G$ for some k. □

Theorem 1.6. *(Wilson's Theorem in a Finite Commutative Group* [M03]*)*
Let $S = \prod_{x \in G} x$.
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 $S = e$.

Proof. As above $S = \prod_{x \in G[2]} x$, and we reduce to the case $G = G[2]$. Now:
a) If G has no elements of order 2, then G is trivial and $S = e$.
b) If G has exactly one element t of order 2, then $G = \{e, t\}$ and $S = et = t$.
c) Suppose G has at least two elements of order 2. By Lemmas 1.4 and 1.5, 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

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

Let $t \in G$ have order 2. By Theorem 1.6, 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 $G = U(n) := U(\mathbb{Z}/n\mathbb{Z})$ be the unit group of the finite ring $\mathbb{Z}/n\mathbb{Z}$. If $n \leq 2$ then $U(n) = \{1\}$ is the trivial group, so certainly $\prod_{x \in U(n)} x = 1$. If $n \geq 3$ then $-1 \neq 1$, so -1 is an order two element of $U(n)$ and the above dichotomy kicks in: $\prod_{x \in U(n)} x = \{\pm 1\}$. When n is prime, $\mathbb{Z}/n\mathbb{Z}$ is a finite *field* so the equation $x^2 = 1$ has no more than the two obvious solutions ± 1. But the equation $x^2 = 1$ may very well have more than two solutions in $\mathbb{Z}/n\mathbb{Z}$ for composite n. E.g. take $n = 8$: 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 two.

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

First one preliminary result: 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 $R_1, \ldots, R_r$, we denote by $\prod_{i=1}^r R_i$ the Cartesian product $R_1 \times R_2 \times \ldots \times R_r$, a ring under coordinatewise addition and multiplication. One sees (immediately) that 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 Cartesian product of commutative groups.

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

Proof. 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 CRT 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 $n = 2^{a_1}$.)
Step 1: The groups $U(1)$ and $U(2)$ are trivial, so the result is clear here. Thus we may assume $n > 2$, so $-1 \in U(n)[2]$ and by Theorem 1.6 $\prod_{x \in U(n)} x = -1$ 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.
Step 2: Suppose $n = p^a$ for an odd prime p 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 the fact that $2 \in U(p^a)$ since p is odd. 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

Namely, Let $n(t) \in \mathbb{Z}/p\mathbb{Z}[t]$ be a polynomial of positive degree, and let $U(n(t)) = U(\mathbb{Z}/p\mathbb{Z}[t]/(n(t)))$. We will compute

$$S_{n(t)} = \prod_{x \in U(n(t))} x.$$

The residue rings $\mathbb{Z}/p\mathbb{Z}[t]/(n(t))$ all have characteristic $p > 2$, so $-1 \neq 1$ and thus as in the classical case (for $n > 2$!) we know by Theorem 1.6 that $S_{n(t)} \in \{\pm 1\}$.

The rings $\mathbb{Z}/p\mathbb{Z}[t]$ and $\mathbb{Z}$ famously have much in common: they both admit a Euclidean algorithm, which has the 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 immediately 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 $p^{d_m+d_n}$. It follows as above that the homomorphism (3) is an isomorphism. An induction argument gives

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

and thus

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

Thus all the work of §2 carries over to this context. We get:

Theorem 3.1. *(Gauss's Theorem in a Polynomial Ring) Let p be an odd prime number, and let $n(t)$ be a monic polynomial of degree at least 1. If $n(t)$ is a power of an irreducible polynomial, then $S_{n(t)} = -1$. Otherwise $S_{n(t)} = 1$.*

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 which have constant term 1 (rather than 0). Thus $U(R_n)$ has order 2^{n-1}.*
a) ($n = 1$): $R_1 = \mathbb{Z}/2\mathbb{Z}$, 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

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

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 $\prod_{x \in U(R_n)} x = 1$.

4. Interlude on cyclicity

Our approach to Gauss's Generalized Wilson Theorem is not the same as Gauss's. In fact he 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 $U(2^a) \cong (\mathbb{Z}/2^{a-2}\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$.

From Theorem 4.1 it follows easily that for $n \geq 3$, $\prod_{x \in U(n)} = -1$ iff $U(n)$ is cyclic iff $n = 4$, p^a or $2p^a$ for an odd prime power p. A generator of $U(n)$ is called a **primitive root** modulo n, so Gauss's results determine the set of n for which primitive roots exist. Theorem 4.1 appears in most elementary number theory texts which develop the theory of congruences, and is one of the most important such results.

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. 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}. 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

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

The reader might like to try to show that for all $p > 2$, $U(\mathbb{Z}/p\mathbb{Z}[t]/(t^2))$ 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 $p(t) \in \mathbb{F}[t]$ be an irreducible polynomial, let $a \in \mathbb{Z}^+$. Then the number of elements of order p in $U(\mathbb{F}[t]/(p(t)^a))$ approaches infinity with a.*

The exact structure of $U(\mathbb{F}[t]/(p(t)^n))$ has been determined by Smith-Gallian [SG85].

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 $G = \prod_{i=1}^r G_{p_i}$.
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]. $\square$

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) 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. 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 F be a field, and let G be a finite subgroup of the group of units $U(F)$ of 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 $x^p = 1$. 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) The characteristic of R divides the order of R.

Proof. a) Left to the reader. b) The characteristic of R is the order of 1 in the additive group $(R, +)$. Apply Lagrange's Theorem. □

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. Then $R/\mathfrak{m}$ is a finite field of order p^{a-b}.
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 that f is surjective. In general, $U(f)$ need not be surjective: consider for instance the quotient map $q : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ for a prime $p > 3$. However, suppose R is finite and local. Then R is primary, so $R \setminus U(R)$ consists of nilpotent elements, and if $y \in U(S)$ and $x \in R$ is such that $f(x) = y$, then x cannot be nilpotent. For if $x^n = 0$ for some $n \in \mathbb{Z}^+$, then $y^n = f(x^n) = f(x)^n = 0$, contradicting the fact that y is a unit. Thus:

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.*

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

Theorem 5.10. *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 generalizes the result that for an odd prime power p^a, $\prod_{x \in U(p^a)} x = -1$. And we can use the same argument: since R has odd order, it has odd characteristic and thus $-1 \neq 1$ give two elements of $U(R)[2]$. Let $x \in R$ be such that $x^2 = 1$. Then $(x+1)(x-1) = 0$. If $x+1, x-1$ both lie in $\mathfrak{m}$ then so does $(x+1) - (x-1) = 2$, which is a contradiction: since R has odd characteristic, $2 \in U(R)$. So one of $x+1$, $x-1$ is a unit, and thus not a zero divisor in R. Since $(x+1)(x-1) = 0$, if $x+1 \in U(R)$ then $x-1 = 0$ and $x = 1$; similarly if $x-1 \in U(R)$ then $x+1 = 0$ and $x = -1$. By Theorem 1.6 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 two and $\prod_{x \in U(R)} x = 1$. □

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}. Since R is local, the surjective homomomorphism $R \to R/\mathfrak{m}$ 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. Thus for any odd prime number p, by Lemma 5.9 we have that $U(q)$ induces 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 $2^a - 2^b$ has odd order iff $b = 0$ iff $\mathfrak{m} = (0)$ iff R is a finite field. Thus:

Proposition 5.11. *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 5.12. *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 $u(\mathbb{Z}[t]/\langle 2t, t^2 - 2\rangle) = -1$.

Proof. a) See [Gi63]. b) The ring $R = \mathbb{Z}[t]/\langle 2t, t^2 - 2\rangle$ has eight elements, represented by $0, 1, 2, 3, t, t+1, t+2, t+3$. We have $U(R) = \{1, 3, t+1, t+3\}$ and

$$u(R) = \prod_{x \in R} x = 1 \cdot 3 \cdot (t+1) \cdot (t+3) = 3(t^2+4t+3) = -(t^2-1) = -(2-1) = -1. \ \square$$

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

Theorem 5.13. *(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 $\mathbb{Z}[t]/\langle 4, 2t, t^2 - 2\rangle$ 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 $U(R) = U(R_i) = 1$.

Remark 5.14. *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 $u(R) = -1$.*

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 positive integers n satisfying the congruence $(n-1)! \equiv -1 \pmod{n}$. Indeed, for $n \in \mathbb{Z}^+$, put

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

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) Working in $\mathbb{Z}/4\mathbb{Z}$ we have $(4-1)! = 6 = 2$. c) Case 1: If $n = p^2$ for a prime number p then necessarily $p > 2$, so $2p < p^2$ and thus $p^2 \mid p \cdot 2p \mid (p^2 - 1)!$ Case 2: If $n \neq p^2$ for a prime number p, then there are integers a, b with $1 < a < b < n$ and $ab = n$ (we may take a to be the smallest divisor of n among integers greater than 1), so $ab \mid (ab - 1)!$ □

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

But there was one outlying case: in the ring $\mathbb{Z}/4\mathbb{Z}$, 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. First one preliminary result.

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 one of the following rings: $\mathbb{Z}/p^2\mathbb{Z}$, a finite field, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}[t]/(t^2)$.

Proof. a) The subring generated by 1 must be all of R (e.g. look at the additive group: a group of prime order has no nontrivial proper subgroups).
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 $t \mapsto t - r$. □

Theorem 6.4. *Let R be a nonzero ring which 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 $\mathbb{Z}/2\mathbb{Z}[t]/(t^2)$.
(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 which 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. Complements

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

Wilson's Theorem is named after the 18th century British mathematician John Wilson. As for many other results in this 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. The result also appeared 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 1.6 was first proved by the early American group theorist G.A. Miller [M03]. However, it is hard to be confident of this given how many times this result has been rediscovered and published in the research literature, e.g. [VW58], [Oh77], [D09]. But I have not been able to find this result in any standard textbook. Perhaps this is because, to the *cognoscenti*, it is irresistible to begin by using Theorem 5.1 to write $G[2] \cong \prod_{i=1}^r (\mathbb{Z}/2\mathbb{Z}, +)$. This paper grew out of a conversation with my colleague Ted Shifrin about how this proof was unfortunately not accessible to our undergraduates. I hope that the more elementary proof given in §1 allows this natural, useful result to be discussed in undergraduate courses.

Vandiver-Weaver proved a generalization of Theorem 1.6 [VW58, Thm. 4.4.9]. Let G be a finite commutative group of order $2n$, and let m be an element of G. Then the map $\iota : G \to G$ by $x \mapsto \frac{m}{x}$ satisfies $\iota^2 = 1_G$. Let f be the number of fixed points of ι, and let t be any order two element of G. Then $\prod_{x \in G} x = m^n t^{\frac{f}{2}}$.

The tools Gilmer uses to prove Theorem 5.12a) are Theorems 5.8 and 4.1. Several other proofs have been given, some extending the result to infinite rings [Ay69], [EF67], [PS70]. Theorem 5.13 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 abitrary 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 rings in which every ideal is principal.[1] That fifty years elapsed between [Gi63] and [HM13] seems very strange. But better late than never. Our proof of Theorem 5.13 is different from Hirano-Matsuoka's and perhaps more broadly accessible: it leans more heavily on group theory than ring theory.

I have not encountered Theorem 6.4 in the literature, 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] which asserts that 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 divsor, 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.

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

[1]It follows from the classification of Theorem 5.12 that if R is a finite ring with cyclic unit group then every ideal in R is principal. It would be interesting to establish this directly and thus reduce Gilmer's Theorem to the Lassak-Dalawat 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 7.1. *(Cyclicity Criterion) Let G be a (not necessarily commutative) finite group. If for all $d \in \mathbb{Z}^+$, $\#\{x \in G \mid x^d = e\} \leq d$, 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

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

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 7.1 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]. It also shares this feature with the proofs which 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. We resist this temptation...for now.

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`

[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.

[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.

[M03] G.A. Miller, *A new proof of the generalized Wilson's theorem*. Ann. of Math. (2) 4 (1903), 188–190.

[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.

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

[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.