

A Presentation: **On A Theorem of Frobenius: Solutions to $x^n = 1$ in Finite Groups** by I.M. Isaacs and G.R. Robinson

Sara Jensen and David Dynerman
Dept. of Mathematics - University of Wisconsin

March 2nd & 9th, 2009

This is a writeup of a talk given in two parts on the above mentioned paper by I.M. Isaacs and G.R. Robinson [6]. It contains some original exposition and additional comments, but otherwise closely follows the content of the original paper.

This talk is about a theorem of Frobenius from 1907 [2] (although Frobenius proved it least as early as 1893). The statement is: Given a finite group G , if an integer n divides $|G|$, then n divides the number of elements $x \in G$ that satisfy $x^n = 1$.

Many proofs of this theorem are known, most of them using character theory, although Frobenius's proof [2] did not. Brauer (1969) [1] and M. Hall (1959) [3] also provided more elementary proofs.

P. Hall (1936) [4] provided a number of very wide generalizations (e.g. whole systems of equations).

We begin this talk by introducing a bit of notation.

- Let G represent a finite group.
- We write $f_n(G) = |\{x \in G : x^n = 1\}|$.
- p will always represent a prime number
- For $n > 0$, n_p will always denote the largest power of the prime p dividing n .

Example. $36_2 = 4$ and $36_3 = 9$.

We begin our discussion with the proof of a basic result from group theory that correlates each group element $g \in G$ with an ordered pair of $x, y \in G$. For this we will need a lemma:

Lemma 0. If $g \in G$ such that $o(g) = mn$ where m and n are coprime, there exists a unique decomposition of $g = xy$ where $x, y \in G$, $xy = yx$ and where $o(x)|n$ and $o(y)|m$.

Before we begin the proof of this lemma, we would like to note that although the lemma is stated generally, there are specific values for m and n which will concern us throughout this talk, and this is when $n = p^b$ for some prime p and n is a number not divisible by p .

Proof. We begin this proof with a number theoretic result; if m and n are any coprime natural numbers, then there exists $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Let $S = \{am + bn : a, b \in \mathbb{Z}\}$, and write s to denote the smallest positive number represented in S . This means that we may write $s = am + bn$ for some $a, b \in \mathbb{Z}$. We wish to show that $s = 1$; it suffices to show that s divides m and s divides n . As m and n are coprime, this implies that a common divisor must be equal to one. Using the division algorithm, we may write $m = qs + r$, where $0 \leq r < s$. Writing s as a linear combination of m and n we obtain:

$$m = qs + r \implies m = q(am + bn) + r \implies (1 - aq)m - bqn = r$$

This shows that $r \in S$. As r must be non-negative and s is the smallest positive element in S , we must have that $r = 0$, showing that s divides m . An analogous argument shows that s divides n , and the result follows.

We now return to our proof of Lemma 0. Fix $g \in G$ where $o(g) = mn$, where m and n are coprime. Now write:

$$g^1 = g^{am+bn} = g^{am}g^{bn} = (g^m)^a(g^n)^b$$

As $x = (g^m)^a$ and $y = (g^n)^b$ are elements of the cyclic group generated by g , it is clear that they commute. We must check that $o((g^m)^a) | n$ and that $o((g^n)^b) | m$. Now by Lagrange's theorem, since $(g^m)^n = 1$, the order of g^m divides n . Yet $o(x)$ must divide $o(g^m)$, so the order of x must also divide n . The proof that $o(y)$ divides m is virtually identical.

Finally, we must show that the x and y found above are unique. So suppose that there exist x', y' such that $g = x'y'$, $x'y' = y'x'$, and $o(x') | n$ and $o(y') | m$. Note that x' and y' commute with g since $g = y'x' \rightarrow x'g = gx'$. Therefore x' and y' commute with all powers of g such as our original x and y . We may therefore conclude that $xy = x'y'$ and that $x'^{-1}x = y'y^{-1}$. We wish to show that the order of $y'y^{-1} = 1$. Note that $(y'y^{-1})^m = 1$, so $o(y'y^{-1})$ divides m . Also, $(y'y^{-1})^n = (x'^{-1}x)^n = 1$, so $o(y'y^{-1})$ divides n . But m and n are coprime, so the only possible number for this order is one. Therefore $y' = y$ and $x' = x$. □

We now begin concentrating on the specific case of coprime numbers where one of them is a power of p and the other is relatively prime to p . The next lemma we present uses this bijection between group elements and pairs of group elements with the form found in Lemma 0. The following lemma is essential to our argument.

Lemma 1. Given a group G , integer n , and prime p , write $q = n_p$ and let T be a set of representatives for those conjugacy classes of elements $y \in G$ such that $y^{n/q} = 1$. Then

$$f_n(G) = \sum_{t \in T} |G : \mathbf{C}_G(t)| f_q(\mathbf{C}_G(t)).$$

Before beginning the proof, let's dissect what this theorem is saying.

- Rather than counting $f_n(G)$ directly by examining every individual group element $g \in G$, it suffices to examine ordered pairs of elements with the properties as described in lemma 0.

- Rather than examine all ordered pairs with this property, it suffices to select representatives from the conjugacy classes of G satisfying the properties of Lemma 0, as conjugacy is going to preserve all of the necessary properties.

Proof. Begin by associating an element $g \in G$ with the ordered pair (x, y) where $x \in \mathbf{C}_G(y)$. As the orders of x, y are relatively prime and x and y commute, we have that $o(g) = o(x)o(y)$. To see this, note that $o(x)|o(g)$ and $o(y)|o(g)$ since x, y are powers of g . Also, $o(x)$ and $o(y)$ are coprime, so $o(x)o(y)|o(g)$. For the other direction, let $m = o(x)o(y)$. Then $g^m = (xy)^m = x^m y^m$ since x and y commute. But $x^m = 1$ and $y^m = 1$, so $g^m = 1$ and thus $o(g)|o(x)o(y)$. Therefore these two quantities are equal.

We next claim that $g^n = 1$ if and only if $x^q = 1$ and $y^{n/q} = 1$. The tricky direction of the if and only if statement is $g^n = 1$ implies that $x^q = 1$ and $y^{n/q} = 1$. So suppose that $g^n = 1$. We may write $n = q(n/q)$. We then have:

$$g^n = 1 \rightarrow (xy)^n = 1 \rightarrow x^n y^n = 1 \rightarrow (x^q)^{n/q} (y^{n/q})^q = 1$$

If $x^q, y^{n/q} \neq 1$, then we have that $(x^q)^{n/q}$ is the inverse of the element $(y^{n/q})^q$. Yet this cannot happen as $o(x^q)$ is relatively prime to $o(y^{n/q})$, and inverses have equal orders.

It therefore follows that:

$$f_n(G) = \sum_{y \in G: y^{n/q}=1} f_q(\mathbf{C}_G(y))$$

However, note that all essential properties in this sum are properties which are preserved via conjugation; that is, if x and y are conjugate to x' and y' , then if $xy = yx$ it follows that $x'y' = y'x'$. Additionally, conjugation is a group automorphism so it also preserves order. So if we let G act on itself via conjugation, we see that for each conjugacy class such that $y^{n/q} = 1$, we may simply pick a representative t from such a conjugacy class and count the number of solutions to $f_q(\mathbf{C}_G(t))$; this number then represents the number of solutions to all $|G : \mathbf{C}_G(t)|$ members of the conjugacy class. We then obtain the result of the lemma, that

$$f_n(G) = \sum_{t \in T} |G : \mathbf{C}_G(t)| f_q(\mathbf{C}_G(t)).$$

□

With the result of this lemma, we now proceed with the proof of Frobenius' theorem by first establishing the result for all powers of primes. For this, we introduce a new bit of notation:

- We say that G has *p-Frobenius property* if for a prime p , every power q of p that divides $|G|$ divides $f_q(G)$.
- “One prime at a time” (Johnny Cash, anyone)?

Lemma 2. Let q be a power of p dividing $|G|$, and suppose $H \subseteq G$ is a subgroup of G satisfying the p -Frobenius property. Then q divides $|G : H| f_q(H)$.

Proof. Note that if q divides the order of H , then q divides $f_q(H)$, so we are done. Therefore we will assume that q does not divide the order of H , and let $q_0 = |H|_p$ (Recall the n_p notation noted at the beginning of the paper).

We claim that $f_q(H) = f_{q_0}(H)$. Certainly, every solution to $f_{q_0}(H)$ is a solution to $f_q(H)$. Additionally, we cannot have a solution to $f_q(H)$ which is not a solution to $f_{q_0}(H)$ or else we would have an element of H of order greater than q_0 , which contradicts LaGrange.

Our next claim is that $|G : H|$ is divisible by $|G|_p/q_0$. Let $p^b = |G|_p$. Then $|G : H| = |G|/|H| = \frac{p^{bl}}{q_0^k}$. This is enough to finish our proof; we have that $\frac{|G|_p}{q_0}$ divides $|G : H|$, which implies that $|G|_p$ divides $|G : H|q_0$, and this quantity divides $|G : H|f_q(H)$. Therefore q , which divides $|G|_p$, also divides $|G : H|f_q(H)$ by transitivity. □

Our final lemma is one from group theory that is perhaps familiar. However, we include it for completeness.

Lemma 3. The number of elements of order m in any group G is a multiple of $\phi(m)$, where ϕ is Euler's phi function.

Proof. Define an equivalence relation on G by setting $x \equiv y$ if $\langle x \rangle = \langle y \rangle$. Check that this is indeed an equivalence relation, and note that elements in the same equivalence class have equal orders. If that order is m , we then know that the cardinality of the class is $\phi(m)$. Then the number of elements in G of order m is the number of equivalence classes containing elements of order m . □

Now we proceed to the theorem that connects the previous lemmas, and the p-Frobenius property.

Theorem 4. Let G be any finite group. Then G has the p -Frobenius property. That is, if q is any p -power, and q divides $|G|$, then q divides $f_q(G)$.

Proof. We proceed by induction on $|G|$. The base case is trivial (If $|G| = 1$, then $f_n(G) = 1$ for any n and the result follows).

Let q be a p -power with q dividing $|G|$. We want to show that q divides $f_q(G)$. We consider two separate cases.

First, suppose that $q = |G|_p$, that is q is the largest p -power that divides $|G|$. Now, let $n = |G|$. Note that $f_n(G) = |G|$ since every element in the group raised to the $|G|$ power is equal to 1 (Why? Every element in the group has order dividing $|G|$)

Applying Lemma 1 using our n and q , we have

$$|G| = f_n(G) = \sum_{t \in T} |G : \mathbb{C}_G(t)| f_q(\mathbb{C}_G(t))$$

Note that some t may lie in $Z(G)$.

$$f_n(G) = \sum_{t \in T \cap Z(G)} |G : \mathbb{C}_G(t)| f_q(\mathbb{C}_G(t)) + \sum_{t \in T - Z(G)} |G : \mathbb{C}_G(t)| f_q(\mathbb{C}_G(t))$$

Remember that we're summing over conjugacy classes. If t is a central element, then it sits in its own conjugacy class, so if $t \in \mathbb{Z}(G)$ we have: $\mathbb{C}_G(t) = G$, $|G : \mathbb{C}_G(t)| = 1$. Now we have

$$f_n(G) = |T \cap \mathbb{Z}(G)|f_q(G) + \sum_{t \in T - \mathbb{Z}(G)} |G : \mathbb{C}_G(t)|f_q(\mathbb{C}_G(t))$$

Now, note that in the sum on the right, each $t \notin \mathbb{Z}(G)$, so $\mathbb{C}_G(t) < G$. This means we can apply the inductive hypothesis, which tells us that $\mathbb{C}_G(t)$ has the p -Frobenius property. Now, by applying Lemma 2, we have q dividing each $|G : \mathbb{C}_G(t)|f_q(\mathbb{C}_G(t))$ term, so q divides the right hand sum.

Next, by assumption, q divides $|G|$, so q divides $|T \cap \mathbb{Z}(G)|f_q(G)$.

Why? Suppose that $a = b + c$ and that $p|a$ and $p|b$. Then we have $pa_0 = pb_0 + c$ for some a_0, b_0 . But by factoring we have $p(a_0 - b_0) = c$, so p divides c as well.

We want to show that q divides $f_q(G)$, so it will suffice to show that p does not divide $|T \cap \mathbb{Z}(G)|$.

By definition, $T \cap \mathbb{Z}(G) = \{y \in \mathbb{Z}(G) | y^{n/q} = 1\}$. (Details: Each element in the set T is conjugate to an element y such that $y^{n/q} = 1$. This implies that $t^{n/q} = 1$, so the set $T \cap \mathbb{Z}(G)$ is just central elements whose n/q power is 1)

Now, $T \cap \mathbb{Z}(G) \subseteq \mathbb{Z}(G)$. By construction, y has order coprime to p , so since all the elements in $T \cap \mathbb{Z}(G)$ are isomorphic images of y , they are central elements whose order is coprime to p .

Thus, by Cauchy's theorem, p does not divide $|T \cap \mathbb{Z}(G)|$ (otherwise $T \cap \mathbb{C}(G)$ would have an element of order p).

We now know that if $q = |G|_p$ and if q divides $|G|$, q divides $f_q(G)$. Now, suppose q is a p -power that divides $|G|$ with $q < |G|_p$. We wish to show that q divides $f_q(G)$.

Let's write $s = f_{|G|_p}(G) - f_q(G)$. By our work above, we know that $|G|_p | f_{|G|_p}(G)$, and since q divides $|G|_p$, we have q dividing $f_{|G|_p}(G)$. By a similar trick as above, if we can show that q divides s , we'll have q dividing $f_q(G)$.

What is s ? Well, write $|G|_p = p^b$ and $q = p^c$. We have $p^b > p^c$. Then s is the difference between the number of solutions to the equation $x^{p^b} = 1$ and $x^{p^c} = 1$. However, note that a solution to the equation $x^{p^c} = 1$ is also a solution to $x^{p^b} = 1$ ($x^{p^b} = (x^{p^c})^{b/c} = 1^{b/c} = 1$), so what we're really counting is the number of elements with p -power order strictly greater than $q = p^c$. In other words, we're counting elements x which solve $x^{p^b} = 1$, but didn't quite make it there by the $q = p^c$ cutoff.

Lemma 3 tells us that the number of elements in G with order p^e is a multiple of $\phi(p^e) = (p - 1)p^{e-1}$.

Why? All numbers less than p^e will be relatively prime except for multiples tp where $tp \leq p^e$. This implies that $t \leq p^{e-1}$, so the number of valid multipliers t is p^{e-1} . So the set $1, 2p, \dots, tp$ has p^{e-1} elements and those are the only elements not coprime to p^e . Thus we have $\phi(p^e) = p^e - p^{e-1} = (p - 1)p^{e-1}$.

Returning, we have $\phi(p^e) = (p - 1)p^{e-1}$, so if $p^e > q$, the biggest q can be is p^{e-1} , so we have q dividing $\phi(p^e)$, and thus q divides s .

Since q divides both $f_{|G|_p}(G)$ and s , we conclude that q divides $f_q(G)$. □

Using all this machinery, we finally have reached our goal

Theorem 5 (Frobenius). Suppose that n divides $|G|$. Then n divides $f_n(G)$.

Proof. Note that it suffices to prove that for each prime p , $q = n_p$ divides $f_n(G)$.

Why? Example: If $n = 3^2 \cdot 5^3 \cdot 7$, it's enough to show that 3^2 , 5^3 and 7 all divide $f_n(G)$.

Let p be a prime, and let $q = n_p$ (Note - if p does not divide $|G|$, then $n_p = 1$, so we're OK). By Lemma 1, we have

$$f_n(G) = \sum_{t \in T} |G : \mathbb{C}_G(t)| f_q(t)$$

By Theorem 4, each $\mathbb{C}_G(t)$ satisfies the p -Frobenius property. Now, applying Lemma 2 we find that q divides each of $|G : \mathbb{C}_G(t)| f_q(t)$ terms, so we conclude that q divides $f_n(G)$. \square

We note that Frobenius' Theorem is often stated in one of two more general forms:

Theorem 5.5. For any integer n and group G , $\gcd(n, |G|)$ divides $f_n(G)$

Proof. Let $d = \gcd(n, |G|)$. Note that by definition d will always divide $|G|$, so by Theorem 5 we have d dividing $f_d(G)$.

We claim that $f_d(G) = f_n(G)$: Suppose we have g that satisfies $g^d = 1$, then $g^n = 1$ as well. Conversely, suppose that $g^n = 1$. Note that $g^{|G|} = 1$ (this is true for any group element in a finite group). Thus the order of g divides both n and $|G|$, so it must divide d . We conclude that $g^d = 1$. \square

Next, suppose we want to count not only solutions of $x^n = 1$, but also $x^n = a$ for some $a \in G$.

Theorem 6. For every choice of $a \in G$ and any positive integer n , the number $f_n(G, a)$ is divisible by $\gcd(n, |\mathbb{C}_G(a)|)$.

Proof. A sketch of the proof is in Isaacs & Robinson [6], which we refer the reader to with the following additional comments:

Starting with any G we can instead work in $G_0 = \mathbb{C}_G(a)$ (since if $\gcd(n, |\mathbb{C}_G(a)|)$ divides $f_n(G_0)$ it will divide $f_n(G)$ as well).

Working in G_0 has the nice property that $a \in \mathbb{Z}(G_0)$. Then, we can only worry about the case where n is a power of p , and then further reduce to where a is a p -element in $\mathbb{Z}(G)$. For further details, see Isaacs & Robinson [6]. \square

Whenever we have an inequality - n dividing $f_n(G)$ in this case - it's interesting to ask what happens when $n = f_n(G)$. In fact, for a while this led to the Frobenius Conjecture:

Suppose that $f_n(G) = n$, then the set of solutions in G to $x^n = 1$ form a (normal) subgroup of G .

The general proof requires the classification of simple groups (Iiyori & Yamaki, 1991) [5], but many cases can also be handled with simpler arguments:

1. The smallest $f_n(G)$ can be for any group is 1 (the identity is the solution for any n).
2. Suppose $f_n(G) = n$ is a p -power for some p . Then the set of solutions to $x^n = 1$ sit inside a Sylow p -subgroup of G and in fact form a subgroup.
3. Suppose $n = 6$ and $n \mid |G|$. So 3 divides $|G|$, so we have at least 3 elements in a subgroup of order 3 (one element by Cauchy, it's inverse and the identity), and the 6th power of each of these elements is equal to 1. Then, since $n = 6$ there can only be one subgroup of order 2, so that subgroup is characteristic and normal and the product of these two subgroups is the desired subgroup.
4. Suppose $n = p \cdot q$. Without loss, suppose that $q > p$. Let Q and P be subgroups of order q and p respectively. If P is the unique subgroup of order p , it's normal and QP is the group we're looking for. If not, then Q permutes P to another subgroup of order p via the conjugation action. The size of the orbit of P has to divide $|G|$. If the orbit is trivial, that means that Q is in the normalizer of P , so QP is a subgroup. If the orbit is non-trivial, the smallest it can be is q . All the subgroups of order $|p|$ intersect trivially, so this accounts for $q(p - 1)$ elements of order p . Each of these elements is a solution to $g^n = 1$. Additionally, the group Q gives us q solutions, so we already have $qp - q + q = qp$ solutions, which is the most we can have. We conclude that Q is the unique subgroup of order q , so QP is the desired subgroup.

References

- [1] Richard Brauer, *On A Theorem of Frobenius*, The American Mathematical Monthly **76** (1969), no. 1, 12–15.
- [2] G. Frobenius, *Über einen Fundamentalsatz der Gruppentheorie, II.*, Sitzungsberichte der Preussischen Akademie Weissenstein (1907), 428–437.
- [3] M. Hall, *Theory of Groups*, Macmillan, 1959.
- [4] P. Hall, *On a Theorem of Frobenius*, Proceedings of the London Mathematical Society **s2-40** (1936), no. 1, 468–501.
- [5] Nobuo Iiyori and Hiroyoshi Yamaki, *On a conjecture of Frobenius*, Bulletin of the American Mathematical Society (New Series) **25** (1991), no. 2, 413–416.
- [6] I. M. Isaacs and G. R. Robinson, *On a Theorem of Frobenius: Solutions of $x^n = 1$ in Finite Groups*, The American Mathematical Monthly **99** (1992), no. 4, 352–354.