Automorphism groups

Gerhardt Hinkle

Missouri State University REU, 2013
Automorphisms

- For a group $G$, an automorphism of $G$ is a function $f : G \to G$ that is bijective and satisfies $f(xy) = f(x)f(y)$ for all $x, y \in G$. 

Introduction

Automorphisms

Original problem

Generalizations

Prime difference

Prime square difference

Possible differences

Further research
Automorphisms

- For a group $G$, an automorphism of $G$ is a function $f : G \to G$ that is bijective and satisfies $f(xy) = f(x)f(y)$ for all $x, y \in G$.
- The set of automorphisms of $G$ forms a group under function composition. The automorphism group of $G$ is written $Aut(G)$. 
Automorphisms

- For a group $G$, an automorphism of $G$ is a function $f : G \rightarrow G$ that is bijective and satisfies $f(xy) = f(x)f(y)$ for all $x, y \in G$.

- The set of automorphisms of $G$ forms a group under function composition. The automorphism group of $G$ is written $\text{Aut}(G)$.

- The inner automorphism group of $G$, written $\text{Inn}(G)$, is the group of automorphisms of the form $f_g(x) = gxg^{-1}$ for a fixed $g \in G$. 
Automorphisms

- For a group $G$, an automorphism of $G$ is a function $f : G \to G$ that is bijective and satisfies $f(xy) = f(x)f(y)$ for all $x, y \in G$.
- The set of automorphisms of $G$ forms a group under function composition. The automorphism group of $G$ is written $Aut(G)$.
- The inner automorphism group of $G$, written $Inn(G)$, is the group of automorphisms of the form $f_g(x) = gxg^{-1}$ for a fixed $g \in G$.
- The center of $G$, written $Z(G)$, comprises those elements of $G$ that commute with every element of $G$. 
Automorphisms

- For a group $G$, an automorphism of $G$ is a function $f : G \rightarrow G$ that is bijective and satisfies $f(xy) = f(x)f(y)$ for all $x, y \in G$.
- The set of automorphisms of $G$ forms a group under function composition. The automorphism group of $G$ is written $\text{Aut}(G)$.
- The inner automorphism group of $G$, written $\text{Inn}(G)$, is the group of automorphisms of the form $f_g(x) = gxg^{-1}$ for a fixed $g \in G$.
- The center of $G$, written $Z(G)$, comprises those elements of $G$ that commute with every element of $G$.
- $\text{Inn}(G) \cong G/Z(G)$
Automorphisms

- For a group $G$, an automorphism of $G$ is a function $f : G \rightarrow G$ that is bijective and satisfies $f(xy) = f(x)f(y)$ for all $x, y \in G$.
- The set of automorphisms of $G$ forms a group under function composition. The automorphism group of $G$ is written $Aut(G)$.
- The inner automorphism group of $G$, written $Inn(G)$, is the group of automorphisms of the form $f_g(x) = gxg^{-1}$ for a fixed $g \in G$.
- The center of $G$, written $Z(G)$, comprises those elements of $G$ that commute with every element of $G$.
- $Inn(G) \cong G/Z(G)$
- $G/Z(G)$ is the group of left cosets of $Z(G)$ in $G$ (i.e. sets of the form $gZ(G)$ for some $g \in G$). It can also be thought of as taking $G$ and setting every element of $Z(G)$ equal to the identity element $e$. 

Automorphism groups

Introduction
- Automorphisms
- Original problem

Generalizations
- Prime difference
- Prime square difference
- Possible differences

Further research
Automorphisms

- For a group $G$, an automorphism of $G$ is a function $f : G \rightarrow G$ that is bijective and satisfies $f(xy) = f(x)f(y)$ for all $x, y \in G$.
- The set of automorphisms of $G$ forms a group under function composition. The automorphism group of $G$ is written $Aut(G)$.
- The inner automorphism group of $G$, written $Inn(G)$, is the group of automorphisms of the form $f_g(x) = gxg^{-1}$ for a fixed $g \in G$.
- The center of $G$, written $Z(G)$, comprises those elements of $G$ that commute with every element of $G$.
- $Inn(G) \cong G/Z(G)$
- $G/Z(G)$ is the group of left cosets of $Z(G)$ in $G$ (i.e. sets of the form $gZ(G)$ for some $g \in G$). It can also be thought of as taking $G$ and setting every element of $Z(G)$ equal to the identity element $e$.
- $|Inn(G)|$ divides $|Aut(G)|$ and $|G|$. 
Cyclic groups

- For a positive integer $n$, the cyclic group of order $n$, written $\mathbb{Z}_n$, is the group of order $n$ generated by one element. It is isomorphic to the group of the integers under addition mod $n$. 

Fundamental theorem of finite abelian groups: Every finite abelian group is isomorphic to the direct product of some number of cyclic groups.

If $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. 

$\phi(n)$ is Euler's totient function, which gives the number of positive integers less than or equal to $n$ that are relatively prime to $n$.
Cyclic groups

For a positive integer $n$, the cyclic group of order $n$, written $\mathbb{Z}_n$, is the group of order $n$ generated by one element. It is isomorphic to the group of the integers under addition mod $n$.

$\mathbb{Z}_n \cong \langle a | a^n = 1 \rangle$
Cyclic groups

- For a positive integer \( n \), the cyclic group of order \( n \), written \( \mathbb{Z}_n \), is the group of order \( n \) generated by one element. It is isomorphic to the group of the integers under addition mod \( n \).
  \[ \mathbb{Z}_n \cong \langle a \mid a^n = 1 \rangle \]
- \( \text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times \), where \( \mathbb{Z}_n^\times \) is the group of the integers relatively prime to \( n \) under multiplication mod \( n \).
Cyclic groups

- For a positive integer \( n \), the cyclic group of order \( n \), written \( \mathbb{Z}_n \), is the group of order \( n \) generated by one element. It is isomorphic to the group of the integers under addition mod \( n \).

\[ \mathbb{Z}_n \cong \langle a | a^n = 1 \rangle \]

- \( \text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times \), where \( \mathbb{Z}_n^\times \) is the group of the integers relatively prime to \( n \) under multiplication mod \( n \).

\[ |\text{Aut}(\mathbb{Z}_n)| = \phi(n) \]
Cyclic groups

- For a positive integer $n$, the cyclic group of order $n$, written $\mathbb{Z}_n$, is the group of order $n$ generated by one element. It is isomorphic to the group of the integers under addition mod $n$.

\[ \mathbb{Z}_n \cong \langle a | a^n = 1 \rangle \]

- $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$, where $\mathbb{Z}_n^\times$ is the group of the integers relatively prime to $n$ under multiplication mod $n$.

\[ |\text{Aut}(\mathbb{Z}_n)| = \phi(n) \]

- $\phi(n)$ is Euler’s totient function, which gives the number of positive integers less than or equal to $n$ that are relatively prime to $n$. 

$\phi(n)$ is Euler’s totient function, which gives the number of positive integers less than or equal to $n$ that are relatively prime to $n$. 

Fundamental theorem of finite abelian groups: Every finite abelian group is isomorphic to the direct product of some number of cyclic groups. 

If $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. 

\[ |\text{Aut}(\mathbb{Z}_n)| = \phi(n) \]
Cyclic groups

- For a positive integer $n$, the cyclic group of order $n$, written $\mathbb{Z}_n$, is the group of order $n$ generated by one element. It is isomorphic to the group of the integers under addition mod $n$.
- $\mathbb{Z}_n \cong \langle a | a^n = 1 \rangle$
- $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$, where $\mathbb{Z}_n^\times$ is the group of the integers relatively prime to $n$ under multiplication mod $n$.
- $|\text{Aut}(\mathbb{Z}_n)| = \phi(n)$
- $\phi(n)$ is Euler’s totient function, which gives the number of positive integers less than or equal to $n$ that are relatively prime to $n$.
- Fundamental theorem of finite abelian groups: Every finite abelian group is isomorphic to the direct product of some number of cyclic groups.
Cyclic groups

- For a positive integer $n$, the cyclic group of order $n$, written $\mathbb{Z}_n$, is the group of order $n$ generated by one element. It is isomorphic to the group of the integers under addition mod $n$.
- $\mathbb{Z}_n \cong \langle a | a^n = 1 \rangle$
- $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$, where $\mathbb{Z}_n^\times$ is the group of the integers relatively prime to $n$ under multiplication mod $n$.
- $|\text{Aut}(\mathbb{Z}_n)| = \phi(n)$
- $\phi(n)$ is Euler’s totient function, which gives the number of positive integers less than or equal to $n$ that are relatively prime to $n$.
- Fundamental theorem of finite abelian groups: Every finite abelian group is isomorphic to the direct product of some number of cyclic groups.
- If $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. 
Original problem

For a group $G$, define $d(G) = |Aut(G)| - |G|$. Prove that $d(G) = 0$ occurs infinitely often, prove that $d(G) = 1$ never occurs, and characterize when $d(G) = -1$. 
Original problem

- For a group $G$, define $d(G) = |\text{Aut}(G)| - |G|$. Prove that $d(G) = 0$ occurs infinitely often, prove that $d(G) = 1$ never occurs, and characterize when $d(G) = -1$.

- If $n \neq 2, 6$, then $\text{Aut}(S_n) \cong S_n$. Therefore, $d(S_n) = 0$ for all $n \neq 2, 6$. 
Original problem (continued)

\[ d(G) = |\text{Aut}(G)| - |G| = \pm 1 \]
Original problem (continued)

- \( d(G) = |Aut(G)| - |G| = \pm 1 \)
- Because \( |Inn(G)| \) divides \( |Aut(G)| \) and \( |G| \), it must divide \( \pm 1 \), so \( |Inn(G)| = 1 \). Therefore, \( |G| = |Z(G)| \), so \( G \) is abelian.
Original problem (continued)

- $d(G) = |\text{Aut}(G)| - |G| = \pm 1$
- Because $|\text{Inn}(G)|$ divides $|\text{Aut}(G)|$ and $|G|$, it must divide $\pm 1$, so $|\text{Inn}(G)| = 1$. Therefore, $|G| = |Z(G)|$, so $G$ is abelian.
- $G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$
Original problem (continued)

- \( d(G) = |\text{Aut}(G)| - |G| = \pm 1 \)

- Because \(|\text{Inn}(G)|\) divides \(|\text{Aut}(G)|\) and \(|G|\), it must divide \(\pm 1\), so \(|\text{Inn}(G)| = 1\). Therefore, \(|G| = |Z(G)|\), so \(G\) is abelian.

- \( G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}} \)

- \( \text{Aut}(G) \geq \text{Aut}(\mathbb{Z}_{p_1^{a_1}}) \times \text{Aut}(\mathbb{Z}_{p_2^{a_2}}) \times \ldots \times \text{Aut}(\mathbb{Z}_{p_k^{a_k}}) \)
Original problem (continued)

- \( d(G) = |Aut(G)| - |G| = \pm 1 \)
- Because \(|Inn(G)|\) divides \(|Aut(G)|\) and \(|G|\), it must divide \(\pm 1\), so \(|Inn(G)| = 1\). Therefore, \(|G| = |Z(G)|\), so \(G\) is abelian.
- \( G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}} \)
- \( Aut(G) \geq Aut(\mathbb{Z}_{p_1^{a_1}}) \times Aut(\mathbb{Z}_{p_2^{a_2}}) \times \ldots \times Aut(\mathbb{Z}_{p_k^{a_k}}) \)
- \( |Aut(\mathbb{Z}_{p_i^{a_i}})| = p_i^{a_i-1}(p_i - 1) \)
Original problem (continued)

- \( d(G) = |\text{Aut}(G)| - |G| = \pm 1 \)
- Because \(|\text{Inn}(G)| \) divides \(|\text{Aut}(G)| \) and \(|G|\), it must divide \( \pm 1 \), so \(|\text{Inn}(G)| = 1 \). Therefore, \(|G| = |Z(G)|\), so \( G \) is abelian.
- \( G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times ... \times \mathbb{Z}_{p_k^{a_k}} \)
- \( \text{Aut}(G) \geq \text{Aut}(\mathbb{Z}_{p_1^{a_1}}) \times \text{Aut}(\mathbb{Z}_{p_2^{a_2}}) \times ... \times \text{Aut}(\mathbb{Z}_{p_k^{a_k}}) \)
- \( |\text{Aut}(\mathbb{Z}_{p_i^{a_i}})| = p_i^{a_i-1}(p_i - 1) \)
- \( a_1 = a_2 = ... = a_k = 1 \)
Original problem (continued)

- \( d(G) = |Aut(G)| - |G| = \pm 1 \)
- Because \( |Inn(G)| \) divides \( |Aut(G)| \) and \( |G| \), it must divide \( \pm 1 \), so \( |Inn(G)| = 1 \). Therefore, \( |G| = |Z(G)| \), so \( G \) is abelian.

- \( G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times ... \times \mathbb{Z}_{p_k^{a_k}} \)
- \( Aut(G) \geq Aut(\mathbb{Z}_{p_1^{a_1}}) \times Aut(\mathbb{Z}_{p_2^{a_2}}) \times ... \times Aut(\mathbb{Z}_{p_k^{a_k}}) \)
- \( |Aut(\mathbb{Z}_{p_i^{a_i}})| = p_i^{a_i - 1}(p_i - 1) \)
- \( a_1 = a_2 = ... = a_k = 1 \)
- \( G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times ... \times \mathbb{Z}_{p_k} \)
Original problem (continued)

▶ What if two of the primes are the same?
Original problem (continued)

- What if two of the primes are the same?
- Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$. 

Original problem (continued)

- What if two of the primes are the same?
- Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$.
- $|Aut(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$
Original problem (continued)

- What if two of the primes are the same?
- Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$.
- $|\text{Aut} (\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$
- Then, $p$ divides $|\text{Aut}(G)|$ and $|G|$, a contradiction.
Original problem (continued)

- What if two of the primes are the same?
- Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$.
- $|Aut(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$
- Then, $p$ divides $|Aut(G)|$ and $|G|$, a contradiction.
- Therefore, $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k}$ for distinct primes $p_1, p_2, \ldots, p_k$. 
What if two of the primes are the same?

Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$.

$|Aut(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$

Then, $p$ divides $|Aut(G)|$ and $|G|$, a contradiction.

Therefore, $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$ for distinct primes $p_1, p_2, \ldots, p_k$.

$|G| = p_1 p_2 \ldots p_k$ and

$|Aut(G)| = (p_1 - 1)(p_2 - 1)\ldots(p_k - 1)$
Original problem (continued)

- What if two of the primes are the same?
- Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$.
- $|Aut(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$
- Then, $p$ divides $|Aut(G)|$ and $|G|$, a contradiction.
- Therefore, $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k}$ for distinct primes $p_1, p_2, \ldots, p_k$.
- $|G| = p_1p_2\ldots p_k$ and 
  $|Aut(G)| = (p_1 - 1)(p_2 - 1)\ldots(p_k - 1)$
- $|Aut(G)| < |G|$, so $|Aut(G)| - |G| = 1$ is impossible.
Original problem (continued)

- What if two of the primes are the same?
- Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$.
- $|\text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$
- Then, $p$ divides $|\text{Aut}(G)|$ and $|G|$, a contradiction.
- Therefore, $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k}$ for distinct primes $p_1, p_2, \ldots, p_k$.
- $|G| = p_1p_2\ldots p_k$ and $|\text{Aut}(G)| = (p_1 - 1)(p_2 - 1)\ldots(p_k - 1)$
- $|\text{Aut}(G)| < |G|$, so $|\text{Aut}(G)| - |G| = 1$ is impossible.
- If $(p_1 - 1)(p_2 - 1)\ldots(p_k - 1) - p_1p_2\ldots p_k = -1$, then $k = 1$. 
Original problem (continued)

- What if two of the primes are the same?
- Suppose $G \geq \mathbb{Z}_p \times \mathbb{Z}_p$.
- $|\text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$
- Then, $p$ divides $|\text{Aut}(G)|$ and $|G|$, a contradiction.
- Therefore, $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k}$ for distinct primes $p_1, p_2, \ldots, p_k$.
- $|G| = p_1 p_2 \ldots p_k$ and $|\text{Aut}(G)| = (p_1 - 1)(p_2 - 1)\ldots(p_k - 1)$
- $|\text{Aut}(G)| < |G|$, so $|\text{Aut}(G)| - |G| = 1$ is impossible.
- If $(p_1 - 1)(p_2 - 1)\ldots(p_k - 1) - p_1 p_2 \ldots p_k = -1$, then $k = 1$.
- Therefore, $d(G) = 1$ is impossible, and $d(G) = -1$ if and only if $G \cong \mathbb{Z}_p$ for some prime $p$. 
Generalizations

- What groups give \( d(G) = \pm p \)?
Generalizations

- What groups give \( d(G) = \pm p \)?
- What groups give \( d(G) = \pm p^2 \)?
Generalizations

- What groups give \( d(G) = \pm p \)?
- What groups give \( d(G) = \pm p^2 \)?
- What values of \( d(G) \) are possible?
Prime difference

\[ d(G) = |Aut(G)| - |G| = \pm p \]
Prime difference

- $d(G) = |Aut(G)| - |G| = \pm p$
- $|Inn(G)| = 1, p$
Prime difference

- $d(G) = |\text{Aut}(G)| - |G| = \pm p$
- $|\text{Inn}(G)| = 1, p$
- The only group of order $p$ is $\mathbb{Z}_p$, but it is impossible for $G/Z(G)$ to be a nontrivial cyclic group.
Prime difference

- $d(G) = |Aut(G)| - |G| = \pm p$
- $|Inn(G)| = 1, p$
- The only group of order $p$ is $\mathbb{Z}_p$, but it is impossible for $G/Z(G)$ to be a nontrivial cyclic group.
- Therefore, $|Inn(G)| = 1$, so $G$ is abelian.
Prime difference

- \( d(G) = |Aut(G)| - |G| = \pm p \)
- \(|Inn(G)| = 1, p \)
- The only group of order \( p \) is \( \mathbb{Z}_p \), but it is impossible for \( G/Z(G) \) to be a nontrivial cyclic group.
- Therefore, \(|Inn(G)| = 1\), so \( G \) is abelian.
- By a similar argument to the \( d(G) = \pm 1 \) case, all prime factors must be distinct and have exponent 1, except that there could be either two \( p \)s or one \( p^2 \) (but not both).
Prime difference

- \( d(G) = |\text{Aut}(G)| - |G| = \pm p \)
- \( |\text{Inn}(G)| = 1, p \)
- The only group of order \( p \) is \( \mathbb{Z}_p \), but it is impossible for \( G/Z(G) \) to be a nontrivial cyclic group.
- Therefore, \( |\text{Inn}(G)| = 1 \), so \( G \) is abelian.
- By a similar argument to the \( d(G) = \pm 1 \) case, all prime factors must be distinct and have exponent 1, except that there could be either two \( p \)s or one \( p^2 \) (but not both).
- Possible cases: \( (q_1, q_2, \ldots q_k \text{ distinct primes not equal to } p) \)
Prime difference

- $d(G) = |Aut(G)| - |G| = \pm p$
- $|Inn(G)| = 1, p$
- The only group of order $p$ is $\mathbb{Z}_p$, but it is impossible for $G/Z(G)$ to be a nontrivial cyclic group.
- Therefore, $|Inn(G)| = 1$, so $G$ is abelian.
- By a similar argument to the $d(G) = \pm 1$ case, all prime factors must be distinct and have exponent 1, except that there could be either two $p$s or one $p^2$ (but not both).
- Possible cases: $(q_1, q_2, ... q_k$ distinct primes not equal to $p$)
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k}$
Prime difference

- ▶ $d(G) = |Aut(G)| - |G| = \pm p$
- ▶ $|Inn(G)| = 1, p$
- ▶ The only group of order $p$ is $\mathbb{Z}_p$, but it is impossible for $G/Z(G)$ to be a nontrivial cyclic group.
- ▶ Therefore, $|Inn(G)| = 1$, so $G$ is abelian.
- ▶ By a similar argument to the $d(G) = \pm 1$ case, all prime factors must be distinct and have exponent 1, except that there could be either two $p$s or one $p^2$ (but not both).
- ▶ Possible cases: ($q_1, q_2, \ldots q_k$ distinct primes not equal to $p$)
  - ▶ $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
  - ▶ $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
Prime difference

- $d(G) = |Aut(G)| - |G| = \pm p$
- $|Inn(G)| = 1, p$
- The only group of order $p$ is $\mathbb{Z}_p$, but it is impossible for $G/Z(G)$ to be a nontrivial cyclic group.
- Therefore, $|Inn(G)| = 1$, so $G$ is abelian.
- By a similar argument to the $d(G) = \pm 1$ case, all prime factors must be distinct and have exponent 1, except that there could be either two $p$s or one $p^2$ (but not both).
- Possible cases: $(q_1, q_2, \ldots q_k$ distinct primes not equal to $p$)
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
  - $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
Prime difference

- \( d(G) = |Aut(G)| - |G| = \pm p \)
- \( |Inn(G)| = 1, p \)
- The only group of order \( p \) is \( \mathbb{Z}_p \), but it is impossible for \( G/Z(G) \) to be a nontrivial cyclic group.
- Therefore, \( |Inn(G)| = 1 \), so \( G \) is abelian.
- By a similar argument to the \( d(G) = \pm 1 \) case, all prime factors must be distinct and have exponent 1, except that there could be either two \( p \)s or one \( p^2 \) (but not both).
- Possible cases: \((q_1, q_2, ... q_k \) distinct primes not equal to \( p \))
  - \( G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k} \)
  - \( G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k} \)
  - \( G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k} \)
  - \( G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k} \)
Prime difference (continued)

\[ G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \]
Prime difference (continued)

\[ G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \]

\[ (q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1 q_2 \ldots q_k = \pm p \]
Prime difference (continued)

- $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1 q_2 \ldots q_k = \pm p$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1 q_2 \ldots q_k = -p$
Prime difference (continued)

- $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1 q_2 \ldots q_k = \pm p$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1 q_2 \ldots q_k = -p$
- There is no general form for the solutions, although they appear to exist for all $p$. 

Prime difference (continued)

- $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = \pm p$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = -p$
- There is no general form for the solutions, although they appear to exist for all $p$.
- $k = 2$: $q_1 + q_2 = p + 1$
Prime difference (continued)

- \( G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \((q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = \pm p\)
- \((q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = -p\)
- There is no general form for the solutions, although they appear to exist for all \( p \).
- \( k = 2: \ q_1 + q_2 = p + 1 \)
- Increasing any \( q_i \) increases the magnitude of the difference, so the lower bound for what values of \( p \) can be obtained for a given \( k \) is \( 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p_{k+1} - 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p_{k+1} - 1) \). This can be reversed to get an upper bound on \( k \) for a given \( p \).
Prime difference (continued)

- $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = \pm p$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = -p$
- There is no general form for the solutions, although they appear to exist for all $p$.
- $k = 2$: $q_1 + q_2 = p + 1$
- Increasing any $q_i$ increases the magnitude of the difference, so the lower bound for what values of $p$ can be obtained for a given $k$ is $3 \cdot 5 \cdot 7 \cdot \ldots \cdot p_{k+1} - 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p_{k+1} - 1)$. This can be reversed to get an upper bound on $k$ for a given $p$.
  - $k = 2$: $p \geq 7$
Prime difference (continued)

- $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = \pm p$
- $(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k = -p$
- There is no general form for the solutions, although they appear to exist for all $p$.
- $k = 2$: $q_1 + q_2 = p + 1$
- Increasing any $q_i$ increases the magnitude of the difference, so the lower bound for what values of $p$ can be obtained for a given $k$ is $3 \cdot 5 \cdot 7 \cdot \ldots \cdot p_{k+1} - 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p_{k+1} - 1)$. This can be reversed to get an upper bound on $k$ for a given $p$.
  - $k = 2$: $p \geq 7$
  - $k = 3$: $p \geq 57$
Prime difference (continued)

- \( G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \( (q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1 q_2 \ldots q_k = \pm p \)
- \( (q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1 q_2 \ldots q_k = -p \)
- There is no general form for the solutions, although they appear to exist for all \( p \).
- \( k = 2: \) \( q_1 + q_2 = p + 1 \)
- Increasing any \( q_i \) increases the magnitude of the difference, so the lower bound for what values of \( p \) can be obtained for a given \( k \) is \( 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p_{k+1} - 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p_{k+1} - 1) \). This can be reversed to get an upper bound on \( k \) for a given \( p \).
  - \( k = 2: \) \( p \geq 7 \)
  - \( k = 3: \) \( p \geq 57 \)
  - \( k = 4: \) \( p \geq 675 \)
Prime difference (continued)

- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
Prime difference (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1q_2\ldots q_k = \pm p$
Prime difference (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1q_2\ldots q_k = \pm p$
- $(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1q_2\ldots q_k = -p$
Prime difference (continued)

- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \((p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1q_2\ldots q_k = \pm p\)
- \((p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1q_2\ldots q_k = -p\)
- \(p(q_1q_2\ldots q_k - (q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 1) + (q_1 - 1)(q_2 - 1)\ldots(q_k - 1) = 0\)
Prime difference (continued)

- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)

\[
(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = \pm p
\]

\[
(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = -p
\]

\[
p(q_1 q_2 \ldots q_k - (q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 1) + (q_1 - 1)(q_2 - 1)\ldots(q_k - 1) = 0
\]

- Both terms on the left side are positive, so there is no solution.
Prime difference (continued)

\[ G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \]
Prime difference (continued)

- $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2q_1q_2\ldots q_k = \pm p$
Prime difference (continued)

- \( G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \((p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p\)
- \((p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -p\)
Prime difference (continued)

- $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2q_1q_2\ldots q_k = \pm p$
- $(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2q_1q_2\ldots q_k = -p$
- $(p - 1)(q_1 - 1)(q - 2 - 1)\ldots(q_k - 1) - pq_1q_2\ldots q_k = -1$
Prime difference (continued)

\[ G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \]

\[ (p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p \]

\[ (p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -p \]

\[ (p - 1)(q_1 - 1)(q - 2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = -1 \]

\[ \text{Only possible if } k = 0 \]
Prime difference (continued)

- \( G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \((p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p\)
- \((p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -p\)
- \((p - 1)(q_1 - 1)(q - 2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = -1\)
- Only possible if \( k = 0 \)
- \( G \cong \mathbb{Z}_{p^2} \)
Prime difference (continued)

$G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
Prime difference (continued)

- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \((p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p\)
Prime difference (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p$
- $(p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = \pm 1$
Prime difference (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p$
- $(p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = \pm 1$
- $p = 2$ has no solution, so $p \geq 3$. 
Automorphism groups

Gerhardt Hinkle

Introduction

Automorphisms

Original problem

Generalizations

Prime difference

Prime square difference

Possible differences

Further research

Prime difference (continued)

\[ G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \]

\[ (p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p \]

\[ (p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = \pm 1 \]

\[ p = 2 \text{ has no solution, so } p \geq 3. \]

\[ f(p) = (p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k \mp 1 \]
Prime difference (continued)

- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \((p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p\)
- \((p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = \pm 1\)
- \(p = 2\) has no solution, so \(p \geq 3\).
- \(f(p) = (p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k \pm 1\)
- There are no solutions if \(f(3) > 0\) and \(f'(p) > 0\) for all \(p \geq 3\).
Prime difference (continued)

- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)

- \((p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = \pm p\)

- \((p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = \pm 1\)

- \( p = 2 \) has no solution, so \( p \geq 3 \).

- \( f(p) = (p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k \mp 1\)

- There are no solutions if \( f(3) > 0 \) and \( f'(p) > 0 \) for all \( p \geq 3 \).

- There are no solutions if \( f(3) > 0 \), \( f'(3) > 0 \), and \( f''(p) > 0 \) for all \( p \geq 3 \).
Prime difference (continued)

- $f(3) = 16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \mp 1$
Prime difference (continued)

- \( f(3) = 16(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 3q_1q_2\ldots q_k \mp 1 \)
- \( f'(3) = 20(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k \)
Prime difference (continued)

- \( f(3) = 16(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 3q_1q_2\ldots q_k \equiv 1 \)
- \( f'(3) = 20(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k \)
- \( f''(p) = (6p - 2)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) \)
Prime difference (continued)

- \( f(3) = 16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \mp 1 \)
- \( f'(3) = 20(q_1 - 1)(q_2 - 1)...(q_k - 1) - q_1q_2...q_k \)
- \( f''(p) = (6p - 2)(q_1 - 1)(q_2 - 1)...(q_k - 1) \)
- \( f''(p) > 0 \) for all \( p \geq 3 \) always holds.
Prime difference (continued)

- $f(3) = 16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \pm 1$
- $f'(3) = 20(q_1 - 1)(q_2 - 1)...(q_k - 1) - q_1q_2...q_k$
- $f''(p) = (6p - 2)(q_1 - 1)(q_2 - 1)...(q_k - 1)$
- $f''(p) > 0$ for all $p \geq 3$ always holds.
- No solutions if
  $16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k > 0$, unless
  $16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k = 1$, in which case $d(G) = p$ and $p = 3$
Prime difference (continued)

- \( f(3) = 16(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 3q_1q_2\ldots q_k \mp 1 \)
- \( f'(3) = 20(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k \)
- \( f''(p) = (6p - 2)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) \)
- \( f''(p) > 0 \) for all \( p \geq 3 \) always holds.
- No solutions if
  \[ 16(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 3q_1q_2\ldots q_k > 0, \text{ unless} \]
  \[ 16(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 3q_1q_2\ldots q_k = 1, \text{ in which} \]
  case \( d(G) = p \) and \( p = 3 \)
- If \( 16(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 3q_1q_2\ldots q_k > 0, \) then
  \[ 20(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - q_1q_2\ldots q_k > 0. \]
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \leq 0\]
  (excluding the one previously-mentioned exception).
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \leq 0\]
  (excluding the one previously-mentioned exception).

- \[\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_k}\right) \leq \frac{3}{16}\]
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1) \cdots (q_k - 1) - 3q_1 q_2 \cdots q_k \leq 0\]
  (excluding the one previously-mentioned exception).
- \[
\left(1 - \frac{1}{q_1}\right) \left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right) \leq \frac{3}{16}
\]
- If \(q_1 = 2, 3\), then there are no solutions.
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \leq 0\]
  (excluding the one previously-mentioned exception).

- \[(1 - \frac{1}{q_1})(1 - \frac{1}{q_2})...(1 - \frac{1}{q_k}) \leq \frac{3}{16}\]

- If \(q_1 = 2, 3\), then there are no solutions.

- Minimum value when \(q_1 = 5, q_2 = 7, ..., q_k = p_{k+2}\),
  where \(p_{k+2}\) is the \((k + 2)\)th prime
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \leq 0\]
  (excluding the one previously-mentioned exception).

- \[\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_k}\right) \leq \frac{3}{16}\]

- If \(q_1 = 2, 3\), then there are no solutions.

- Minimum value when \(q_1 = 5, q_2 = 7, \ldots, q_k = p_{k+2}\), where \(p_{k+2}\) is the \((k + 2)\)th prime

- \[\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)\ldots\left(1 - \frac{1}{p_{k+2}}\right) \leq \frac{3}{16}\]
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1)...(q_k - 1) - 3q_1q_2...q_k \leq 0\]
  (excluding the one previously-mentioned exception).

- \[
  \left(1 - \frac{1}{q_1}\right) \left(1 - \frac{1}{q_2}\right) \ldots \left(1 - \frac{1}{q_k}\right) \leq \frac{3}{16}
  \]

- If \(q_1 = 2, 3\), then there are no solutions.

- Minimum value when \(q_1 = 5, q_2 = 7, \ldots, q_k = p_{k+2}\), where \(p_{k+2}\) is the \((k+2)\)th prime

- \[
  \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \ldots \left(1 - \frac{1}{p_{k+2}}\right) \leq \frac{3}{16}
  \]

- \(k \geq 994\)
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 3q_1q_2\ldots q_k \leq 0\]
  (excluding the one previously-mentioned exception).

- \[\left(1 - \frac{1}{q_1}\right) \left(1 - \frac{1}{q_2}\right) \ldots \left(1 - \frac{1}{q_k}\right) \leq \frac{3}{16}\]

- If \(q_1 = 2, 3\), then there are no solutions.

- Minimum value when \(q_1 = 5, q_2 = 7, \ldots, q_k = p_{k+2}\), where \(p_{k+2}\) is the \((k + 2)\)th prime

- \[\left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \ldots \left(1 - \frac{1}{p_{k+2}}\right) \leq \frac{3}{16}\]

- \(k \geq 994\)

- Other possibility: \(k = 993, p = 3, G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \ldots \times \mathbb{Z}_{p_{995}}, \) and \(d(G) = 3\)
  (can be easily confirmed to be false)
Prime difference (continued)

- There are only solutions if
  \[16(q_1 - 1)(q_2 - 1)\cdots(q_k - 1) - 3q_1q_2\cdots q_k \leq 0\]
  (excluding the one previously-mentioned exception).

- \( \left(1 - \frac{1}{q_1}\right) \left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right) \leq \frac{3}{16}\)

- If \( q_1 = 2, 3 \), then there are no solutions.

- Minimum value when \( q_1 = 5, q_2 = 7, \ldots, q_k = p_{k+2} \),
  where \( p_{k+2} \) is the \((k + 2)\)th prime

- \( \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \cdots \left(1 - \frac{1}{p_{k+2}}\right) \leq \frac{3}{16}\)

- \( k \geq 994\)

- Other possibility: \( k = 993, p = 3\),
  \[ G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \cdots \times \mathbb{Z}_{p_{995}}, \text{ and } d(G) = 3\]
  (can be easily confirmed to be false)

- Therefore, a solution to \( d(G) = \pm p \) exists if and only if \( k \geq 994\).
Prime difference (continued)

- We can use a similar manner to find a lower bound on the values of $k$ that give a difference of at least $\pm p_0$. 
Prime difference (continued)

- We can use a similar manner to find a lower bound on the values of $k$ that give a difference of at least $\pm p_0$.

$$\left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \ldots \left(1 - \frac{1}{p_{k+2}}\right) \leq \frac{p_0}{(p_0^2-1)(p_0-1)},$$

where the product excludes the term containing $p_0$ so that there are $k$ terms in total.
Prime difference (continued)

- We can use a similar manner to find a lower bound on the values of $k$ that give a difference of at least $\pm p_0$.

- $(1 - \frac{1}{3})(1 - \frac{1}{5}) \ldots \left(1 - \frac{1}{p_{k+2}}\right) \leq \frac{p_0}{(p_0^2-1)(p_0-1)}$, where the product excludes the term containing $p_0$ so that there are $k$ terms in total.

- The product in the left side of the inequality goes to 0 as $k$ goes to $\infty$, so there will always exist a value of $k$ so that the inequality is satisfied.
Prime difference (continued)

- We can use a similar manner to find a lower bound on the values of $k$ that give a difference of at least $\pm p_0$.
- $(1 - \frac{1}{3}) (1 - \frac{1}{5}) \ldots \left(1 - \frac{1}{p_{k+2}}\right) \leq \frac{p_0}{(p_0^2-1)(p_0-1)}$, where the product excludes the term containing $p_0$ so that there are $k$ terms in total.
- The product in the left side of the inequality goes to 0 as $k$ goes to $\infty$, so there will always exist a value of $k$ so that the inequality is satisfied.
- Let $k(p_0)$ be the lowest value of $k$ satisfying the inequality for a given $p_0$. Then, any group $G$ for which $d(G) = \pm p_0$ must have $k \geq k(p_0)$, except that it could be possible to have $k = k(p_0) - 1$, $\{q_1, q_2, \ldots, q_k\} = \{3, 5, 7, \ldots, p_{k+2}\} \setminus \{p_0\}$, and $d(G) = p_0$. 


Prime difference (continued)

- $k(p_0)$ increases very rapidly.
Prime difference (continued)

- $k(p_0)$ increases very rapidly.
- $k(3) = 994$
Prime difference (continued)

- $k(p_0)$ increases very rapidly.
- $k(3) = 994$
- $k(5)$ is too large to compute easily. (much greater than 20 million)
Prime difference (continued)

- \( k(p_0) \) increases very rapidly.
- \( k(3) = 994 \)
- \( k(5) \) is too large to compute easily. (much greater than 20 million)
- The numbers are so large that the chance of getting \( \pm 1 \) is very remote, so I conjecture that there are no solutions.
Prime square difference

\[ d(G) = |Aut(G)| - |G| = \pm p^2 \]
Prime square difference

- $d(G) = |\text{Aut}(G)| - |G| = \pm p^2$
- $|\text{Inn}(G)| = 1, p, p^2$
Prime square difference

- \[ d(G) = |\text{Aut}(G)| - |G| = \pm p^2 \]
- \[ |\text{Inn}(G)| = 1, p, p^2 \]
- The only group of order \( p \) is \( \mathbb{Z}_p \), and the only groups of order \( p^2 \) are \( \mathbb{Z}_{p^2} \) and \( \mathbb{Z}_p \times \mathbb{Z}_p \).
Prime square difference

- \( d(G) = |\text{Aut}(G)| - |G| = \pm p^2 \)
- \( |\text{Inn}(G)| = 1, p, p^2 \)
- The only group of order \( p \) is \( \mathbb{Z}_p \), and the only groups of order \( p^2 \) are \( \mathbb{Z}_{p^2} \) and \( \mathbb{Z}_p \times \mathbb{Z}_p \).
- \( \text{Inn}(G) \cong \{e\}, \mathbb{Z}_p \times \mathbb{Z}_p \)
Prime square difference

- $d(G) = |Aut(G)| - |G| = \pm p^2$
- $|Inn(G)| = 1, p, p^2$
- The only group of order $p$ is $\mathbb{Z}_p$, and the only groups of order $p^2$ are $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.
- $Inn(G) \cong \{e\}, \mathbb{Z}_p \times \mathbb{Z}_p$
- Either $G$ is abelian or $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. 

**Introductions**

*Automorphisms*

*Original problem*

*Generalizations*

*Prime difference*

*Possible differences*

*Further research*
Abelian

- $d(G) = \pm p^2$, $G$ abelian
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
Automorphism

Introduction

Automorphisms

Gerhardt Hinkle

Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Must be calculated manually
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Must be calculated manually
  - $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
Abelian

- \(d(G) = \pm p^2\), \(G\) abelian
- Possibilities:
  - \(G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}\)
    - Calculated like in the \(d(G) = \pm p\) case; can only give \(d(G) = -p^2\)
  - \(G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}\)
    - Must be calculated manually
  - \(G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}\)
    - No solution
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
  - $G \cong \mathbb{Z}_{p} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Must be calculated manually
  - $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - No solution
  - $G \cong \mathbb{Z}_{p^3} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
    - Must be calculated manually
  - $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
    - No solution
  - $G \cong \mathbb{Z}_{p^3} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$
    - $G \cong \mathbb{Z}_{p^3}$, $d(G) = -p^2$

Further research
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k}$
    - Must be calculated manually
  - $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k}$
    - No solution
  - $G \cong \mathbb{Z}_{p^3} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k}$
    - $G \cong \mathbb{Z}_{p^3}$, $d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k}$
Abelian

- \( d(G) = \pm p^2 \), \( G \) abelian
- Possibilities:
  - \( G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
    - Calculated like in the \( d(G) = \pm p \) case; can only give \( d(G) = -p^2 \)
  - \( G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
    - Must be calculated manually
  - \( G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
    - No solution
  - \( G \cong \mathbb{Z}_{p^3} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
    - \( G \cong \mathbb{Z}_{p^3}, \ d(G) = -p^2 \)
  - \( G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
    - \( k = 1: \ p = 2, \ q_1 = 5, \ d(G) = 4 \)
Abelian

- $d(G) = \pm p^2$, $G$ abelian
- Possibilities:
  - $G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Calculated like in the $d(G) = \pm p$ case; can only give $d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - Must be calculated manually
  - $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - No solution
  - $G \cong \mathbb{Z}_{p^3} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - $G \cong \mathbb{Z}_{p^3}, d(G) = -p^2$
  - $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - $k = 1$: $p = 2, q_1 = 5, d(G) = 4$
    - $k = 2$: $p = 2, q_1 = 5, q_2 = 7, d(G) = 4$
d(G) = ±p^2, G abelian

Possibilities:

- \( G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
  - Calculated like in the \( d(G) = ±p \) case; can only give \( d(G) = -p^2 \)
- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
  - Must be calculated manually
- \( G \cong \mathbb{Z}_p^2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
  - No solution
- \( G \cong \mathbb{Z}_p^3 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
  - \( G \cong \mathbb{Z}_p^3, d(G) = -p^2 \)
- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
  - \( k = 1: p = 2, q_1 = 5, d(G) = 4 \)
  - \( k = 2: p = 2, q_1 = 5, q_2 = 7, d(G) = 4 \)
  - ... (must be calculated manually)
Non-abelian

- $\text{Inn}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$
Non-abelian

\[ \text{Inn}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p \]
\[ G/Z(G) \cong \langle a, b | a^p = b^p = 1, ba = ab \rangle \]
Non-abelian

- $\text{Inn}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$
- $G/Z(G) \cong \langle a, b | a^p = b^p = 1, ba = ab \rangle$
- In $G$, $a^p = x$, $b^p = y$, and $bab^{-1}a^{-1} = z$, where $x, y, z \in Z(G)$. 
Non-abelian

- \( \text{Inn}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p \)
- \( G/Z(G) \cong \langle a, b | a^p = b^p = 1, ba = ab \rangle \)
- In \( G \), \( a^p = x, b^p = y \), and \( bab^{-1}a^{-1} = z \), where \( x, y, z \in Z(G) \).
- There may be some elements of \( Z(G) \) that are unrelated to any of \( a, b, x, y \), and \( z \), but there can’t be any non-central elements of \( G \) that depend on anything but \( a, b \), and elements of \( Z(G) \).
Non-abelian (continued)

\[ G \cong \langle a, b, z \mid a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle \]
Non-abelian (continued)

- \( G \cong \langle a, b, z | a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle \)
- Let \( \phi, \psi, \) and \( \chi \) be automorphisms of \( G \), defined as follows:
Non-abelian (continued)

- $G \cong \langle a, b, z | a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle$

- Let $\phi$, $\psi$, and $\chi$ be automorphisms of $G$, defined as follows:
  - $\phi(a) = a$, $\phi(b) = bz$, $\phi(z) = z$
Non-abelian (continued)

- $G \cong \langle a, b, z | a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle$

- Let $\phi$, $\psi$, and $\chi$ be automorphisms of $G$, defined as follows:
  - $\phi(a) = a$, $\phi(b) = bz$, $\phi(z) = z$
  - $\psi(a) = az$, $\psi(b) = b$, $\psi(z) = z$
Non-abelian (continued)

- $G \cong \langle a, b, z | a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle$

- Let $\phi$, $\psi$, and $\chi$ be automorphisms of $G$, defined as follows:
  - $\phi(a) = a$, $\phi(b) = bz$, $\phi(z) = z$
  - $\psi(a) = az$, $\psi(b) = b$, $\psi(z) = z$
  - $\chi(a) = ab^l$, $\chi(b) = b$, $\chi(z) = z$
Non-abelian (continued)

$G \cong \langle a, b, z | a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle$

Let $\phi$, $\psi$, and $\chi$ be automorphisms of $G$, defined as follows:

$\phi(a) = a, \phi(b) = bz, \phi(z) = z$
$\psi(a) = az, \psi(b) = b, \psi(z) = z$
$\chi(a) = ab^l, \chi(b) = b, \chi(z) = z$

$o(\phi) = o(\psi) = o(\chi) = p, \psi \circ \phi = \phi \circ \psi, \chi \circ \phi \neq \phi \circ \chi, \chi \circ \psi = \psi \circ \chi$
Non-abelian (continued)

- $G \cong \langle a, b, z | a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle$
- Let $\phi$, $\psi$, and $\chi$ be automorphisms of $G$, defined as follows:
  - $\phi(a) = a, \phi(b) = bz, \phi(z) = z$
  - $\psi(a) = az, \psi(b) = b, \psi(z) = z$
  - $\chi(a) = ab^l, \chi(b) = b, \chi(z) = z$
- $o(\phi) = o(\psi) = o(\chi) = p, \psi \circ \phi = \phi \circ \psi, \chi \circ \phi \neq \phi \circ \chi, \chi \circ \psi = \psi \circ \chi$
- $\langle \phi, \psi, \chi \rangle \cong (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$
Non-abelian (continued)

- $G \cong \langle a, b, z | a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle$
- Let $\phi$, $\psi$, and $\chi$ be automorphisms of $G$, defined as follows:
  - $\phi(a) = a$, $\phi(b) = bz$, $\phi(z) = z$
  - $\psi(a) = az$, $\psi(b) = b$, $\psi(z) = z$
  - $\chi(a) = ab^l$, $\chi(b) = b$, $\chi(z) = z$
- $o(\phi) = o(\psi) = o(\chi) = p$, $\psi \circ \phi = \phi \circ \psi$, $\chi \circ \phi \neq \phi \circ \chi$, $\chi \circ \psi = \psi \circ \chi$
- $\langle \phi, \psi, \chi \rangle \cong (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$
- The group generated by $\phi$, $\psi$, and $\chi$ is a subgroup of $\text{Aut}(G)$. 
Non-abelian (continued)

- $G \cong \langle a, b, z | a^{p^k} = b^{p^l} = z^p = 1, ba = abz, za = az, zb = bz \rangle$
- Let $\phi$, $\psi$, and $\chi$ be automorphisms of $G$, defined as follows:
  - $\phi(a) = a$, $\phi(b) = bz$, $\phi(z) = z$
  - $\psi(a) = az$, $\psi(b) = b$, $\psi(z) = z$
  - $\chi(a) = ab^l$, $\chi(b) = b$, $\chi(z) = z$
- $o(\phi) = o(\psi) = o(\chi) = p$, $\psi \circ \phi = \phi \circ \psi$, $\chi \circ \phi \neq \phi \circ \chi$, $\chi \circ \psi = \psi \circ \chi$
- $\langle \phi, \psi, \chi \rangle \cong (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$
- The group generated by $\phi$, $\psi$, and $\chi$ is a subgroup of $Aut(G)$.
- $p^3$ divides $|Aut(G)|$ and $|G|$, so $|Aut(G)| - |G| = \pm p^2$ is impossible.
Non-abelian (continued)

- \( G \cong \langle a, b, z \mid a^{pk} = b^{pl} = z^p = 1, ba = abz, za = az, zb = bz \rangle \)

- Let \( \phi, \psi, \) and \( \chi \) be automorphisms of \( G \), defined as follows:
  - \( \phi(a) = a, \phi(b) = bz, \phi(z) = z \)
  - \( \psi(a) = az, \psi(b) = b, \psi(z) = z \)
  - \( \chi(a) = ab^l, \chi(b) = b, \chi(z) = z \)

- \( o(\phi) = o(\psi) = o(\chi) = p, \psi \circ \phi = \phi \circ \psi, \chi \circ \phi \neq \phi \circ \chi, \chi \circ \psi = \psi \circ \chi \)

- \( \langle \phi, \psi, \chi \rangle \cong (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p \)

- The group generated by \( \phi, \psi, \) and \( \chi \) is a subgroup of \( \text{Aut}(G) \).

- \( p^3 \) divides \( |\text{Aut}(G)| \) and \( |G| \), so \( |\text{Aut}(G)| - |G| = \pm p^2 \) is impossible.

- If there are any other elements in \( Z(G) \), then \( G \) is a direct product of the above group with an abelian group, so \( p^3 \) still divides \( |\text{Aut}(G)| \) and \( |G| \).
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.

- If $G \cong \mathbb{Z}_n$, then $d(G) = \phi(n) - n = -(n - \phi(n))$. 

- $n - \phi(n)$ is called the cototient of $n$.

- Any positive integer that cannot be expressed as $n - \phi(n)$ for any positive integer $n$ is called a noncototient.

- The negatives of some noncototients can still be obtained as $d(G)$ for some noncyclic group $G$.

- e.g. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{385}$, $d(G) = -100$.

- If a noncototient equals $2^p$ for some prime $p$, then I conjecture that $d(G) = -2^p$ is impossible.
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.
- If $G \cong \mathbb{Z}_n$, then $d(G) = \phi(n) - n = -(n - \phi(n))$.
- $n - \phi(n)$ is called the cototient of $n$. 

▶ $n - \phi(n)$ is called the cototient of $n$. 

▶ Any positive integer that cannot be expressed as $n - \phi(n)$ for any positive integer $n$ is called a noncototient.

▶ 10, 26, 34, 50, 52, 58, 86, 100, 116, ...

▶ The negatives of some noncototients can still be obtained as $d(G)$ for some noncyclic group $G$.

▶ e.g. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{385}$, $d(G) = -100$.
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.
- If $G \cong \mathbb{Z}_n$, then $d(G) = \phi(n) - n = -(n - \phi(n))$.
- $n - \phi(n)$ is called the cototient of $n$.
- Any positive integer that cannot be expressed as $n - \phi(n)$ for any positive integer $n$ is called a noncototient.
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.

- If $G \cong \mathbb{Z}_n$, then $d(G) = \phi(n) - n = -(n - \phi(n))$.

- $n - \phi(n)$ is called the cototient of $n$.

- Any positive integer that cannot be expressed as $n - \phi(n)$ for any positive integer $n$ is called a noncototient.
  - 10, 26, 34, 50, 52, 58, 86, 100, 116, ...
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.

- If $G \cong \mathbb{Z}_n$, then $d(G) = \phi(n) - n = -(n - \phi(n))$.

- $n - \phi(n)$ is called the cototient of $n$.

- Any positive integer that cannot be expressed as $n - \phi(n)$ for any positive integer $n$ is called a noncototient.
  - $10, 26, 34, 50, 52, 58, 86, 100, 116, ...$

- The negatives of some noncototients can still be obtained as $d(G)$ for some noncyclic group $G$. 
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.

- If $G \cong \mathbb{Z}_n$, then $d(G) = \phi(n) - n = -(n - \phi(n))$.

- $n - \phi(n)$ is called the cototient of $n$.

- Any positive integer that cannot be expressed as $n - \phi(n)$ for any positive integer $n$ is called a noncototient.
  - 10, 26, 34, 50, 52, 58, 86, 100, 116, ...

- The negatives of some noncototients can still be obtained as $d(G)$ for some noncyclic group $G$.
  - e.g. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{385}$, $d(G) = -100$
Possible differences

- All of the groups that were found in the $d(G) = \pm p$ case had $d(G) = -p$. Therefore, if my conjecture in the last part of that case is true, then $d(G) = p$ is impossible.

- If $G \cong \mathbb{Z}_n$, then $d(G) = \phi(n) - n = -(n - \phi(n))$.

- $n - \phi(n)$ is called the cototient of $n$.

- Any positive integer that cannot be expressed as $n - \phi(n)$ for any positive integer $n$ is called a noncototient.
  - 10, 26, 34, 50, 52, 58, 86, 100, 116, ...

- The negatives of some noncototients can still be obtained as $d(G)$ for some noncyclic group $G$.
  - e.g. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{385}$, $d(G) = -100$

- If a noncototient equals $2p$ for some prime $p$, then I conjecture that $d(G) = -2p$ is impossible.
Noncototent difference

$d(G) = |Aut(G)| - |G| = -2p$, where $2p$ is a noncototent
Noncototient difference

- $d(G) = |Aut(G)| - |G| = -2p$, where $2p$ is a noncototient
- $|Inn(G)| = 1, 2, p, 2p$
Noncototient difference

- $d(G) = |Aut(G)| - |G| = -2p$, where $2p$ is a noncototient
- $|Inn(G)| = 1, 2, p, 2p$
- $Inn(G) \cong \{e\}, D_{2p}$
Noncototient difference

- $d(G) = |Aut(G)| - |G| = -2p$, where $2p$ is a noncototient
- $|Inn(G)| = 1, 2, p, 2p$
- $Inn(G) \cong \{e\}, D_{2p}$
- Either $G$ is abelian or $G/Z(G) \cong D_{2p}$. 
Abelian

- Possible cases:
Abelian

Possible cases:

\[ G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k} \]
Abelian

- Possible cases:
  - \( G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
  - \( 6(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 4q_1q_2\ldots q_k = -2p \)
Abelian

- Possible cases:
  - $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
    - $6(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 4q_1q_2\ldots q_k = -2p$
    - $3(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 2q_1q_2\ldots q_k = -p$
Abelian

Possible cases:

- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
  - $6(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 4q_1q_2\ldots q_k = -2p$
  - $3(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 2q_1q_2\ldots q_k = -p$
  - The left side is even but the right side is odd, so there is no solution.
Abelian

Possible cases:

- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
  - $6(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 4q_1q_2\ldots q_k = -2p$
  - $3(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 2q_1q_2\ldots q_k = -p$
  - The left side is even but the right side is odd, so there is no solution.

- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
Possible cases:

- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
  - $6(q_1 - 1)(q_2 - 1)(q_k - 1) - 4q_1 q_2 \ldots q_k = -2p$
  - $3(q_1 - 1)(q_2 - 1)(q_k - 1) - 2q_1 q_2 \ldots q_k = -p$
  - The left side is even but the right side is odd, so there is no solution.

- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
  - This case has the same problem as the previous case, so there is no solution.
Automorphism groups

Gerhardt Hinkle

Introduction

Automorphisms
Original problem

Generalizations
Prime difference
Prime square difference
Possible differences

Further research

Abelian

Possible cases:

1. \( G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
   - \( 6(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 4q_1q_2\ldots q_k = -2p \)
   - \( 3(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - 2q_1q_2\ldots q_k = -p \)
   - The left side is even but the right side is odd, so there is no solution.

2. \( G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
   - This case has the same problem as the previous case, so there is no solution.
Abelian (continued)

$G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
Abelian (continued)

- \[ G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \]
- \[ (p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -2p \]
Abelian (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -2p$
- $(p^2 - 1)(p-1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = -2$
Abelian (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)...(q_k - 1) - p^2 q_1 q_2 ... q_k = -2p$
- $(p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)...(q_k - 1) - pq_1 q_2 ... q_k = -2$
- The left side is odd unless one of the $q_i$s is 2, so let $q_1 = 2$. 
Abelian (continued)

- \( G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k} \)
- \((p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -2p \)
- \((p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = -2 \)
- The left side is odd unless one of the \( q_i \)s is 2, so let \( q_1 = 2 \).
- \((p^2 - 1)(p - 1)(q_2 - 1)(q_3 - 1)\ldots(q_k - 1) - 2pq_2 q_3 \ldots q_k = -2 \)
Abelian (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2q_1q_2\ldots q_k = -2p$
- $(p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1q_2\ldots q_k = -2$
- The left side is odd unless one of the $q_i$s is 2, so let $q_1 = 2$.
- $(p^2 - 1)(p - 1)(q_2 - 1)(q_3 - 1)\ldots(q_k - 1) - 2pq_2q_3\ldots q_k = -2$
- $r_i = q_{i+1}$
Abelian (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -2p$
- $(p^2 - 1)(p-1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = -2$
- The left side is odd unless one of the $q_i$s is 2, so let $q_1 = 2$.
- $(p^2 - 1)(p - 1)(q_2 - 1)(q_3 - 1)\ldots(q_k - 1) - 2pq_2 q_3 \ldots q_k = -2$
- $r_i = q_{i+1}$
- $(p^2 - 1)(p - 1)(r_1 - 1)(r_2 - 1)\ldots(r_{k-1} - 1) - 2pr_1 r_2 \ldots r_{k-1} = -2$
Abelian (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -2p$
- $(p^2 - 1)(p - 1)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - pq_1 q_2 \ldots q_k = -2$
- The left side is odd unless one of the $q_i$s is 2, so let $q_1 = 2$.
- $(p^2 - 1)(p - 1)(q_2 - 1)(q_3 - 1)\ldots(q_k - 1) - 2pq_2 q_3 \ldots q_k = -2$
- $r_i = q_{i+1}$
- $(p^2 - 1)(p - 1)(r_1 - 1)(r_2 - 1)\ldots(r_{k-1} - 1) - 2pr_1 r_2 \ldots r_{k-1} = -2$
- Using a similar argument as in the last case for $d(G) = \pm p$, the lower bound on $k - 1$ is $k(p)$. 
Abelian (continued)

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \ldots \times \mathbb{Z}_{q_k}$
- $(p^2 - 1)(p^2 - p)(q_1 - 1)(q_2 - 1)\ldots(q_k - 1) - p^2 q_1 q_2 \ldots q_k = -2p$
- $(p^2 - 1)(p-1)(q_1-1)(q_2-1)\ldots(q_k-1) - pq_1 q_2 \ldots q_k = -2$
- The left side is odd unless one of the $q_i$s is 2, so let $q_1 = 2$.
- $(p^2 - 1)(p-1)(q_2-1)(q_3-1)\ldots(q_k-1) - 2pq_2 q_3 \ldots q_k = -2$
- $r_i = q_{i+1}$
- $(p^2 - 1)(p-1)(r_1-1)(r_2-1)\ldots(r_{k-1}-1) - 2pr_1 r_2 \ldots r_{k-1} = -2$
- Using a similar argument as in the last case for $d(G) = \pm p$, the lower bound on $k - 1$ is $k(p)$.
- Therefore, I conjecture that if $2p$ is a noncototient, then there are no abelian groups $G$ for which $d(G) = -2p$. 
Further research

Finish the last case for $d(G) = \pm p$
Further research

- Finish the last case for $d(G) = \pm p$
- Finish the abelian case for $d(G) = -2p$ when $2p$ is a noncototient
Further research

- Finish the last case for $d(G) = \pm p$
- Finish the abelian case for $d(G) = -2p$ when $2p$ is a noncototient
- Do the non-abelian case for $d(G) = -2p$ when $2p$ is a noncototient ($G/Z(G) \cong D_{2p}$)

Further research
Further research

- Finish the last case for \( d(G) = \pm p \)
- Finish the abelian case for \( d(G) = -2p \) when \( 2p \) is a noncototient
- Do the non-abelian case for \( d(G) = -2p \) when \( 2p \) is a noncototient \( (G/Z(G) \cong D_{2p}) \)
- Extend to \( d(G) = \pm p^n, \ d(G) = \pm pq \), etc.
Further research

- Finish the last case for \( d(G) = \pm p \)
- Finish the abelian case for \( d(G) = -2p \) when \( 2p \) is a noncototient
- Do the non-abelian case for \( d(G) = -2p \) when \( 2p \) is a noncototient \( (G/Z(G) \cong D_{2p}) \)
- Extend to \( d(G) = \pm p^n, \ d(G) = \pm pq, \) etc.
- Determine what other differences are possible or impossible