Published in *American Mathematical Monthly* **105** (1998), no. 4, pp. 359–361.

THE NUMBER OF CONJUGACY CLASSES

Michael Reid

Let G be a finite group, $|G|$ its order, and s the number of its conjugacy classes. Burnside [1, p. 295] uses the theory of representations of finite groups to prove that if $|G|$ is odd, then $|G| \equiv s \bmod 16$. He also gives as an exercise [1, p. 320] that if every prime p dividing $|G|$ satisfies $p \equiv 1 \bmod 4$, then $|G| \equiv s \bmod 32$. Poonen [4] gives an elementary proof (i.e. without using representation theory) of a generalization of the latter statement. Specifically, Poonen shows that if $m > 1$, and every prime p dividing $|G|$ satisfies $p \equiv 1 \bmod m$, then $|G| \equiv s \bmod 2m^2$.

The purpose of this note is to prove another congruence along the same lines, and to show we have obtained the strongest possible results. We introduce some notation. For $m \geq 1$, let $\mathcal{G}_m$ denote the collection of all finite groups G such that every prime p dividing $|G|$ satisfies $p \equiv 1 \bmod m$. Let $B(m)$ denote the greatest common divisor of $|G| - s$, over all G in $\mathcal{G}_m$. Then the above results are reformulated as:

Theorem. (Burnside) *$B(2)$ is divisible by 16.*

Theorem. (Poonen) *If $m > 1$, then $B(m)$ is divisible by $2m^2$.*

These results are strengthened slightly by the following observation.

Remark. If $m > 1$, then any prime $p \equiv 1 \bmod m$ is necessarily odd. Therefore $\mathcal{G}_m \subseteq \mathcal{G}_2$, so $B(m)$ is divisible by $B(2)$, and thus by 16.

If $m > 2$, we can say slightly more about $B(m)$. In this case, we obtain the desired result under a weaker hypothesis. This result is an easy exercise using representation theory; see for example [5]. Here we give an elementary proof, using Poonen's technique.

Proposition. *If $|G|$ is not divisible by 3, then $|G| \equiv s \bmod 3$.*

Proof. Poonen [4] shows that the set $A = \{(x, y) \in G^2 \mid xy \neq yx\}$ has cardinality $|G|(|G| - s)$. The set A is clearly in bijection with $B = \{(x, y, z) \in G^3 \mid xyz = 1 \neq zyx\}$ by $(x, y) \mapsto (x, y, (xy)^{-1})$. Now B supports the order 3 permutation $(x, y, z) \mapsto (y, z, x)$, which has no fixed points. Therefore $|B| = |G|(|G| - s)$ is divisible by 3, from which the proposition follows. $\square$

Corollary. *If $m > 2$, then $B(m)$ is divisible by 3.*

The corollary, along with the theorems of Burnside and Poonen, gives the strongest possible results about $B(m)$. This is the content of the following theorem.

Theorem. *If $m > 2$, then $B(m)$ is the least common multiple of 48 and $2m^2$. Also $B(2) = 16$ and $B(1) = 1$.*

Proof. For $m > 2$, let $B'(m) = \mathrm{LCM}(48, 2m^2)$. The corollary and the theorems of Burnside and Poonen show that $3, 16$ and $2m^2$ each divide $B(m)$. Therefore, their least common multiple, $B'(m)$, divides $B(m)$. For a prime p, let G_p denote the non-abelian group

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}/p^2\mathbb{Z} \text{ and } a \equiv 1 \bmod p \right\}$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX

of order p^3. The center of G_p is

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G_p \;\middle|\; a \equiv 1 \bmod p^2 \text{ and } b \equiv 0 \bmod p \right\},$$

which has order p. The reader can easily verify that the conjugacy class of a non-central element $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ is

$$\left\{ \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \in G_p \;\middle|\; a' \equiv a \bmod p^2 \text{ and } b' \equiv b \bmod p \right\},$$

which has size p. Therefore G_p has $s_p = p^2 + p - 1$ conjugacy classes, p of size 1 and $p^2 - 1$ of size p. Note also that $|G_p| - s_p = (p+1)(p-1)^2$. For a prime q, let v_q denote the q-adic valuation, so $v_q(n)$ is the largest integer e such that q^e divides n. We will compare $v_q(B(m))$ and $v_q(B'(m))$. Consider several cases.

Case 1. Suppose $q \nmid m$ and $q \neq 2, 3$. By Dirichlet's theorem on primes in arithmetic progressions (and the Chinese remainder theorem), there is a prime p with $p \equiv 1 \bmod m$ and $p \equiv 2 \bmod q$. Then $v_q(B(m)) \leq v_q(|G_p| - s_p) = v_q((p+1)(p-1)^2) = 0 = v_q(B'(m))$.

Case 2. Suppose $3 = q \nmid m$. There is a prime p with $p \equiv 1 \bmod m$ and $p \equiv 2 \bmod 9$. Then $v_3(B(m)) \leq v_3((p+1)(p-1)^2) = 1 = v_3(B'(m))$.

Case 3. Suppose $2 = q \nmid m$. There is a prime p with $p \equiv 1 \bmod m$ and $p \equiv 3 \bmod 8$. Then $v_2(B(m)) \leq v_2((p+1)(p-1)^2) = 4 = v_2(B'(m))$.

Case 4. Suppose $2 \neq q | m$. Let $e = v_q(m)$. There is a prime p with $p \equiv 1 \bmod m$ and $p \equiv 1 + q^e \bmod q^{e+1}$. Then $v_q(B(m)) \leq v_q((p+1)(p-1)^2) = 2e = v_q(B'(m))$.

Case 5. Suppose $2 = q | m$. Let $e = v_2(m)$. If $e = 1$, there is a prime p with $p \equiv 1 \bmod m$ and $p \equiv 3 \bmod 8$. Then $v_2(B(m)) \leq v_2((p+1)(p-1)^2) = 4 = v_2(B'(m))$. If $e \geq 2$, there is a prime p with $p \equiv 1 \bmod m$ and $p \equiv 1 + 2^e \bmod 2^{e+1}$. Then $v_2(B(m)) \leq v_2((p+1)(p-1)^2) = 2e + 1 = v_2(B'(m))$.

This shows that for every prime q, we have $v_q(B(m)) \leq v_q(B'(m))$. Therefore $B(m) = B'(m)$, so the first statement is proved. For the second statement, note that $B(2)$ divides $|G_3| - s_3 = 16$, so $B(2) = 16$. Also, $B(1)$ divides both $|G_3| - s_3 = 16$ and $|G_2| - s_2 = 3$, so $B(1) = 1$. $\square$

Several authors (e.g. [2, 3, 5]) have considered a similar problem with a different type of hypothesis, namely that the order of G is divisible only by some finite set of primes, $p_1, p_2, \ldots, p_r$. Hirsch [2] also gives an elementary, but more complicated proof of our Proposition. The strongest result under this type of hypothesis appears to be Mann's theorem [3, p. 83], from which it follows easily that $\mathrm{LCM}(48, 2m^2)$ divides $B(m)$ for $m > 2$. It would be interesting to know if Mann's result is the best possible under this type of hypothesis.

Acknowledgment.
I am grateful to the referee for bringing some of the references to my attention.

References

1. W. Burnside, *Theory of Groups of Finite Order*, Second Edition, University Press, Cambridge, 1911.
2. K. A. Hirsch, *On a theorem of Burnside*, The Quarterly Journal of Mathematics, Oxford, Second Series **1** (1950), 97–99. MR 12,156a
3. Avinoam Mann, *Conjugacy classes in finite groups*, Israel Journal of Mathematics **31** (1978), no. 1, 78–84. MR 58 #22296
4. Bjorn Poonen, *Congruences Relating the Order of a Group to the Number of Conjugacy Classes*, American Mathematical Monthly **102** (1995), no. 5, 440–442.
5. R. W. van der Waall, *On a theorem of Burnside*, Elemente der Mathematik **25** (1970), 136–137.

Old address:

Michael Reid

Current address:

Michael Reid

Department of Mathematics
Box 1917
Brown University
Providence, RI 02912
U.S.A.
reid@math.brown.edu

Department of Mathematics
University of Central Florida
Orlando, FL 32816
U.S.A.
reid@cflmath.com