On one-relator quotients of the modular group

George Havas
Centre for Discrete Mathematics and Computing
School of Information Technology and Electrical Engineering
The University of Queensland, Queensland 4072, Australia.
Email: havas@itee.uq.edu.au

joint work with
Marston Conder, University of Auckland, NZ
Mike Newman, ANU, Canberra

This research was partially supported by the Australian Research Council.

Groups St Andrews, Bath, 11 August 2009

Introduction

The modular group is a much studied object in mathematics.

Indeed in the 2009 Abel Prize documentation for Gromov's award this group is described as
"one of the most important groups in the modern history of mathematics".

It has standard representations as a group of geometric transformations and as a group of matrices.

It is (isomorphic to) the projective special linear group PSL$(\mathbf{2}, \boldsymbol{Z})$.

It is SQ-universal.

It has a large collection of interesting quotients.

This includes most of the nonabelian finite simple groups.

We study the modular group as a finitely presented group.

It is isomorphic to the free product of the cyclic groups C_2 and C_3 and has natural and shortest presentation: $\{x, y \mid x^2, y^3\}$.

We investigate the question: what are the one-relator quotients of this group?

We are happy when we can either give the order of the group when finite or a proof of infiniteness otherwise.

If we can tell you the order, we can tell you its structure.

How can we determine the order of a finite FP-group?

Favorite tool: coset enumeration.

How can we prove a group to be infinite?

Simplest method: abelian quotient invariants of it or one of its subgroups reveals it.

More complicated study of the group itself: cohomology; geometry; graphical; rewriting (Knuth-Bendix); prove infinitely many different properties (eg, quotients), Golod-Shafarevich, . . .

Or any of the above for a subgroup, quotient or section.

So, which groups can we obtain by adding one extra relator $w(x, y)$ to the standard presentation?

Many interesting cases are already known, including infinite sequences.

Triangle groups: $(xy)^n$ — infinite for $n \geq 6$ (GA Miller 1902)

Generalized triangle groups: w^n — almost all infinite
(Baumslag, Morgan, Shalen 1987, HMT95, LRS95: only 8 finite)

Finite simple groups $\boldsymbol{PSL(2,m)}$: − for prime $\boldsymbol{m \geq 5}$
(Campbell and Robertson, 1980; $\boldsymbol{2m+5}$ syllables $\boldsymbol{u = xy}$, $\boldsymbol{v = xy^{-1}}$):

$$\boldsymbol{u^2 v u^{(m-3)/2} v u^2 v u^{(3m-3)/2} v}$$

Finite soluble groups (Campbell, Heggie, Robertson and Thomas 1992):

$$\boldsymbol{xy^{-1}xy(xyxy^{-1})^{n-1}xy^{-1}xy}$$

$\boldsymbol{G(n)}$ is metabelian with order $\boldsymbol{6(n^2+3)}$ if $\boldsymbol{n \neq 3 \bmod 4}$
and has derived length 3 and order $\boldsymbol{12(n^2+3)}$ if $\boldsymbol{n = 3 \bmod 4}$.

The trivial group : ? how many ? (lots)

Work on Schur multipliers gives a necessary condition for a finite 2-generator group to be presentable with 3 relators.

Suffice it to say that a finite $\boldsymbol{\{2,3\}}$-generated group is not presentable as a one-relator quotient of the modular group unless rank$\boldsymbol{(M(G)) = 0}$ or $\boldsymbol{1}$.

One-relator quotients of the modular group have been much considered over time.

Indeed, in 1856 Hamilton produced what we can read as a presentation for A_5 (which he called "Icosian Calculus") via a one-relator quotient of the modular group: $\langle \iota, \kappa, \lambda \mid \iota^2 = 1, \kappa^3 = 1, \lambda^5 = 1, \lambda = \iota\kappa \rangle$.

In 1901 G.A. Miller identified the groups $\langle x, y \mid x^2, y^3, (xy)^n \rangle$ for $n = 2, 3, 4$ and 5 (referring to Burnside (1897)) and in 1902 showed that they are infinite for $n > 5$.

In 1987 Conder substantially identified all 270 one-relator quotients of the modular group, where the extra relator has length up to 24.

Subsequently Ulutaș and Cangül (2004) wrote a paper on this topic.
(Sadly it is neither comprehensive nor fully correct.)

In addition, many successful investigations into efficient presentations for simple groups have specifically studied one-relator quotients of the modular group, dating from 1980.

To better understand the nature of one-relator quotients of the modular group we extend Conder's 1987 work by investigating longer presentations.

We describe a canonical form for them.

In that context, we study all such quotients with extra relator having length up to 36 and determine the order of almost all of them.

Up to equivalence, there are 8326 presentations where the extra relator has length greater than 24.

We confirm Conder's 1987 results and we determine the order of all of the groups, except for seven with length 36.

The presentations of the groups whose order we have not been able to determine provide interesting challenge problems.

When we can determine the order of a finite group, we are able to give detailed structural information about it.

All of our results are based on computer calculations, sometimes substantial.

We use Magma, which provides excellent facilities for our needs.

(Alternatively GAP can be used to do the required computations.)

We provide supplementary materials, including some Magma programs on my website, together with their outputs.

These programs and outputs give some further details on our calculations and also provide information on computer resource usage.

Conder's approach revisited

In 1987 Conder was motivated by a problem about graphs to study what he called at the time "three-relator quotients of the modular group".

We now prefer the term *one-relator*, reflecting the count of extra relators, rather than the total relator count.

Following Conder's ideas but not the detail, we define the modular group $\Gamma = \langle x, y \mid x^2, y^3 \rangle$ and consider its one relator quotient $G = \langle x, y \mid x^2, y^3, w(x, y) \rangle$.

Any non-trivial element (other than x, y or y^{-1}) in Γ is conjugate to an element of the form $xy^{\epsilon_1}xy^{\epsilon_2}\dots xy^{\epsilon_n}$ where $\epsilon_i = \pm 1$.

We consider such elements as candidates for the extra relator and say they have n syllables or length $2n$.

There are 2^n.

However we can significantly reduce the number we look at by utilizing automorphisms of the modular group. We define $u = xy$ and $v = xy^{-1}$.

In Γ, $u^{-1}v = y^{-1}x^{-1}xy^{-1} = y^{-2} = y$ and $vu^{-1}v = xy^{-1}y = x$ so Γ has an alternative presentation $P = \{u, v \mid (vu^{-1}v)^2, (u^{-1}v)^3\}$.

This presentation provides a good environment for describing canonical representatives for the extra relator.

Taking the automorphisms of Γ into account reduces the number of presentations significantly.

Indeed our program reveals:
1, 2, 2, 4, 4, 8, 9, 18, 23, 44, 63, 122, 190, 362, 612, 1162, 2056, 3914, . . .

Do you recognize this?

It is the number of n-bead necklaces (turning over is allowed) where complements are equivalent.

http://www.research.att.com/∼njas/sequences/A000011

$$\left(\ \ 2^{\lfloor n/2 \rfloor} + \Sigma_{d|n}(2^{n/d}\phi(2d))/(2n)\ \ \right)/2$$

Our methods and the easy cases

We have implemented a Magma program which generates (almost) all canonical representatives of extra relators and tries to determine group order.

Our first, quite quick approach, is the following.

Try to enumerate the cosets of the trivial subgroup (using the x, y presentation, defining a maximum of 10^6 cosets using a well-chosen ACE strategy).

If that fails, look at the AQI of all (conjugacy classes of) subgroups with index up to $\mathbf{33}$.

$\mathbf{8569}$ presentations (ex 8596 necklaces): ACE fails to complete for $\mathbf{237}$.

So $\mathbf{8332}$ of these define finite groups (and 7/27 omitted).

Trivial : $\mathbf{1855}$, $\boldsymbol{C_2}$: $\mathbf{2183}$, $\boldsymbol{C_3}$: $\mathbf{681}$, $\boldsymbol{|G| = 6}$: $\mathbf{931}$ $\boldsymbol{(C_6}$: $\mathbf{133}$, $\boldsymbol{S_3}$: $\mathbf{798)}$

Small $\boldsymbol{\{2,3\}}$-generated simple groups:

$\boldsymbol{60 : 23 - A_5}$; $\boldsymbol{168 : 11 - L_2(7)}$; $\boldsymbol{504 : 7 - L_2(8)}$; $\boldsymbol{660 : 3 - L_2(11)}$;
$\boldsymbol{1092 : 7 - L_2(13)}$ $\boldsymbol{2448 : 7 - L_2(17)}$; $\boldsymbol{3420 : 4 - L_2(19)}$; $\boldsymbol{4080 : 3 - L_2(16)}$;

Missing $\boldsymbol{5616 : 0 - L_3(3)}$; shortest has $\mathbf{21}$ syllables

Missing $\boldsymbol{12180 : 0 - L_2(29)}$; shortest has $\mathbf{19}$ syllables

$\mathbf{14880 : 3 - L_2(31)}$; shortest has $\mathbf{17}$ syllables

$\mathbf{39732 : 1 - L_2(43)}$; shortest has $\mathbf{17}$ syllables $\mathbf{(2p + 5 = 91)}$

$\mathbf{1 : 1855,\ 2 : 2183,\ 3 : 681,\ 6 : 931,\ 12 : 242,\ 18 : 92,\ 24 : 171,\ 42 : 193,\ 48 : 148,}$
$\mathbf{54 : 48,\ 60 : 42,\ 72 : 43,\ 78 : 150,\ 96 : 72,}$

$\mathbf{114 : 118,\ 120 : 20,\ 126 : 75,\ 144 : 38,\ 150 : 80,\ 162 : 25,\ 168 : 53,\ 180 : 13,}$
$\mathbf{186 : 66,\ 192 : 10,\ 216 : 18,\ 222 : 51,\ 234 : 31,\ 240 : 20,\ 258 : 37,\ 288 : 10,}$
$\mathbf{294 : 56,\ 312 : 13,\ 324 : 11,\ 336 : 59,\ 342 : 9,\ 360 : 9,\ 366 : 10,\ 378 : 3,\ 384 : 12,}$
$\mathbf{402 : 4,\ 432 : 33,\ 438,\ 486 : 2,\ 504 : 29,\ 576 : 13,\ 624 : 9,\ 648 : 12,\ 660 : 4,}$
$\mathbf{672 : 23,\ 720 : 11,\ 750 : 10,\ 768 : 21,\ 936 : 6,}$

$\mathbf{1008 : 32,\ 1152 : 4,\ 1092 : 8,\ 1200 : 3,\ 1296 : 9,\ 1320 : 9,\ 1368 : 2,\ 1440 : 5,}$
$\mathbf{1512 : 4,\ 1536 : 13,\ 1944 : 5,\ 1980 : 2,\ 2016 : 11,\ 2058 : 2,\ 2160 : 14,\ 2184 : 12,}$
$\mathbf{2304 : 7,\ 2448 : 9,\ 2520,\ 2640 : 15,\ 2736 : 2,\ 2880 : 5,\ 3024 : 2,\ 3072 : 2,\ 3276,}$
$\mathbf{3402,\ 3420 : 4,\ 3456 : 2,\ 3600 : 2,\ 3888 : 5,\ 3960 : 10,\ 4032 : 2,\ 4080 : 3,}$
$\mathbf{4320 : 10,\ 4368 : 9,\ 4378 : 6,\ 4536 : 2,\ 4608 : 2,\ 4680 : 2,\ 5040 : 3,\ 5184,}$

5760 : 4, 5832 : 2, 6000, 6048 : 3, 6072 : 5, 6144 : 9, 6552 : 5, 6840 : 4, 7056 : 4, 7344 : 3, 7500, 7560 : 2, 7800 : 2, 8064, 8400, 8640, 8748, 9000 : 2, 9072, 9792 : 2, 9828,

10260 : 2, 10368, 10752, 11520 : 2, 11160, 11664 : 2, 11880, 12144 : 4, 12288, 13104 : 3, 13320 : 2, 13680 : 4, 14040, 14112 : 2, 14400, 14880 : 3, 15120, 15552 : 4, 17280 : 3, 18432, 18750 : 10, 18816, 19440 : 2, 19656 : 2, 20520, 21168 : 4, 21504 : 2, 24192 : 4, 25200 : 2, 25272, 26208 : 4, 27216 : 4, 27720, 31104, 31680 : 2, 32256 : 5, 32400, 32736, 36864, 38304, 39732, 39366, 42000, 44064, 44640 : 2, 45360, 51840 : 4, 52488, 57456, 61560, 72756, 75924, 77760, 81648, 83160, 84240, 90720 : 2, 97200,

112320, 122760, 123120, 145152, 184860 : 2, 233280, 234000, 278640, 346752, 362880, 367416, 653184, 777600.

Structure of all finite ones easily determined.

237 coset enumerations failed to complete, **171** for good reason.

Their presentations define infinite groups (and our program or theory (GT) provides a proof).

On this laptop: Total time: 773.812 seconds, Total memory usage: 69.20MB.

$\mathbf{66}$ presentations to go.

Try harder.

Lemma. A group is finite if its largest metabelian quotient is finite and it has a cyclic subgroup with finite index.

ACE ($\mathbf{10^7}$ cosets, $\boldsymbol{P(u,v)/\langle v\rangle}$)

LIS ($\boldsymbol{G(x,y)}$, index $\mathbf{33}$ subgroups and subgroup cores with index $\leq \mathbf{2^{15}}$).

$\mathbf{24}$ more finite groups:

Indexes: 1, 3, 4, 13, $64:2$, 516, 588, 3276, 6084, 7392, 8192, 78624, 87500, 98304, 110592, 172032, 292032, 353808, 367416, 403368, 1572864, 3538944, 5308416.

Now harder to determine structure.

24 infinite with proofs; 15 by AQI, 9 GT (also have massive subgroup p-quotients and/or many PSL images).

18 left (1 with 17 syllables, rest with 18).

Try harder again (10^8 cosets; LIS to 55; cores to 2^{16}).

3 more indexes: 31, 712500, 746928; 1 more infinite.

14 left.

Harder work proves 4 of these are infinite, 2 finite.

(Golod-Shafarevich), infinitely many different PSL quotients (Plesken and Fabianska, 2009), and infinite quotient by finding a matrix representation.

Coset enumerations allowing billions of cosets, including:

INDEX = 63824112 (m=814813557 t=814913514) $\mathbf{2^4 3^4 11^3 37}$

INDEX = 36 (m=1038797675 t=1046881197)

What is this group G with cyclic subgroup with index $\mathbf{63824112}$?

Let us play bingo: $|U_3(11)| = \mathbf{70915680} = \mathbf{2^5 3^2 5 11^3 37}$

We started off knowing G has largest soluble quotient with order 18.

We readily find the index 2 subgroup maps onto $U_3(11)$ . . .

Another tidbit. Consider G_{3649} with 20 syllables.

John Cannon showed:

```
Index = 464486400, Total cosets = 464486400.
Order of group is 464486400 = [ <2, 15>, <3, 4>, <5, 2>, <7, 1> ].
Degree of permutation representation is 34560.

Chief factors:-
    G
    |  Cyclic(3)
    *
    |  A(1, 8)                 = L(2, 8)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2) (2 copies)
    *
    |  Cyclic(2) (6 copies)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2) (2 copies)
    *
    |  Cyclic(3)
    *
    |  Cyclic(5) (2 copies)
    1

    CPU time for group 3649 is 52218.620 seconds.
```

[Almost all of the CPUtime goes into constructing the perm rep of degree 34560 from the regular representation.]

The last 8

Length 17

$$u^{10}v^2uvuv^2$$

It is easy to show that $PSL(2,25)$ and $PSL(3,3)$ are images, and under related subgroups we can see 2^{1+12}.

All that has order 358 848 921 600 $= 2^{20}3^4 5^2 13^2$.

Do you recognize this?

It is like the largest known quotient of $(2,3,13;4)$ (Holt and Rees 1999).

Coxeter (1939) defined: $(p,q,r;s) = \langle x,y \mid x^p, y^q, (xy)^r, [x,y]^s \rangle$

Our group is easily seen to be a central extension of $(2,3,13;4)$.

That was all we knew till a couple of weeks ago.

At a meeting in Edinburgh I suggested to Derek that I thought $\mathbf{(2, 3, 13; 4)}$ looked like it should be finite.

So we focussed on proving just that.

And, yes, it is finite and our group is a 2-fold cover.

On to length 18.

$$\#2086 \quad u^4vu^3v^3uv^4uv$$

Its abelian quotient is C_6, which is its largest known quotient.

The derived group is perfect with presentation:

$$bbABAbbaBBa, baaBAAABaab, babaBABABababA$$

We know it does not have any L_2 quotients or any "small" simple quotients.

???

$$\#2507 \quad u^4vuvu^2v^2uvuv^4$$

Maps onto $2 : L_2(19) : 3^2$, whose order is 61560.

$$\#2767 \quad u^4vuv^4u^3vuv^3$$

Sections include 2, 3, 7^8, 19 and $\widehat{L}_2(7)$.
So order is at least 220 814 937 504.

$$\#2878 \quad u^4v^2u^2v^4u^2vuv^2$$

Sections include $\mathbf{2}$, $\mathbf{3}$, $\mathbf{19}$ and $L_2(13)$.
So order is at least 124488.

$$\#3179 \quad u^3vu^2vu^2v^2uv^2uv^3$$

Sections include $\mathbf{3}$, $\mathbf{19}$ and $\widehat{L}_2(13)$.
So order is at least 124488 (same as for #2878, but different structure).

$$\#3405 \quad u^3vu^2v^2uv^3u^2vuv^2$$

Sections include $\mathbf{2}^3$, $\mathbf{3}$, $\mathbf{5}$, $\mathbf{7}$ and $\widehat{L}_2(11)$.
So order is at least 158400.

$$\#3646 \quad u^3vuvuv^3u^2vuvuv^2$$

Sections include $\mathbf{2}$, $\mathbf{3}$, $\mathbf{19}$ and $L_2(64)$.
So order is at least 67616640.

Questions

Why are so many one-relator quotients of the modular group finite?

Are all $\{2, 3\}$-generated simple groups one-relator quotients of the modular group?

Acknowledgements

We are grateful to Shona Yu who did many experimental investigations on this topic during a research project in 2001/2002.

References

W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. Journal of Symbolic Computation, 24:235–265, 1997.
See also `http://www.maths.usyd.edu.au:8000/u/magma/`

C.M. Campbell, G. Havas, A. Hulpke and E.F. Robertson. Efficient simple groups. Communications in Algebra, 31:5191–5197, 2003.

Colin M. Campbell, George Havas, Colin Ramsay and Edmund F. Robertson, 'Nice efficient presentations for all small simple groups and their covers', *LMS J. Comput. Math.* **7** (2004) 266–283.

Colin M. Campbell, George Havas, Colin Ramsay and Edmund F. Robertson, On the efficiency of the simple groups with order less than a and their covers. Experimental Mathematics 16 (2007), 347-358.

C.M. Campbell and E.F. Robertson, ‘A deficiency zero presentation for $SL(2, p)$’, *Bull. London Math. Soc.* **12** (1980) 17–20.

Colin M. Campbell and Edmund F. Robertson, ‘The efficiency of simple groups of order $< 10^5$’, *Comm. Algebra* **10** (1982) 217–225.

Colin M. Campbell and Edmund F. Robertson, ‘Presentations for the simple groups G, $10^5 < |G| < 10^6$’, Comm. Algebra **12** (1984) 2643–2663.

M. Conder. Three-relator quotients of the modular group. Quarterly Journal of Mathematics, Oxford, Second Series, 38:427–447, 1987.

Marston Conder, George Havas and M.F. Newman. *On one-relator quotients of the modular group; supplementary materials* (2009), `http://www.itee.uq.edu.au/~havas/orqmg`

Marston Conder, George Havas and Colin Ramsay, ‘Efficient presentations for the Mathieu simple group M_{22} and its cover’, in *Finite Geometries, Groups, and Computation* (Walter de Gruyter, 2006) 33–42.

H.S.M. Coxeter and W.O.J. Moser, *Generators and relations for discrete groups*,
Springer, Berlin, 1st edition, 1957; 2nd edition, 1965; 3rd edition, 1972; 4th edition, 1979.

The GAP Group, Aachen, St Andrews, *GAP – Groups, Algorithms, and Programming, Version* **4.2**, 2001. See also
`http://www-gap.dcs.st-and.ac.uk/~gap/`

William Rowan Hamilton, Memorandum respecting a new system of roots of unity, Philosophical Magazine, 12 (1856), p. 446.

G. Havas and C. Ramsay. Coset enumeration: ACE version 3.001 (2001). Available as `http://www.itee.uq.edu.au/~havas/ace3001.tar.gz`

A. Jamali and E.F. Robertson, 'Efficient presentations for certain simple groups', *Comm. Algebra* **17** (1989) 2521–2528.

P.E. Kenne, ‘Efficient presentations for three simple groups’, *Comm. Algebra* **14** (1986) 797–800.

G.A. Miller. On the groups generated by two operators. Bull. Amer. Math. Soc. (1901) 424-426.

G.A. Miller. Groups defined by the orders of two generators and the order of their product. Amer. J. Math. 24 (1902), no. 1, 96–100.

Yücel Türker Ulutaş and İsmail Naci Cangül, One relator quotients of the modular group. Bull. Inst. Math. Acad. Sinica 32 (2004), no. 4, 291–296.

J. Wiegold, ‘The Schur multiplier: an elementary approach’, *Groups – St Andrews 1981*, London Mathematical Society Lecture Note Series **71** (Cambridge University Press, Cambridge, 1982) 137–154.

GT = generalized triangle G. Baumslag, J. W. Morgan and P. B. Shalen, Math. Proc. Cambridge Philos. Soc. 102 (1987), no. 1, 25–31; MR0886432 (88g:20062)]

Howie, J.(4-HWAT); Metaftsis, V.(4-HWAT); Thomas, R. M.(4-LSTR-CS) Finite generalized triangle groups. Trans. Amer. Math. Soc. 347 (1995), no. 9, 3613–3623.

Metaftsis, Vasileios(4-HWAT); Miyamoto, Izumi(J-YAMAN-EE) One-relator products of two groups of order three with short relators. Kyushu J. Math. 52 (1998), no. 1, 81–97.