COHOMOLOGY OF BRAIDS, PRINCIPAL CONGRUENCE SUBGROUPS AND GEOMETRIC REPRESENTATIONS

F. CALLEGARO, F. R. COHEN*, AND M. SALVETTI

Abstract. The main purpose of this article is to give the integral cohomology of classical principal congruence subgroups in $SL(2,\mathbb{Z})$ as well as their analogues in the 3-strand braid group with local coefficients in symmetric powers of the natural symplectic representation. The resulting answers (1) correspond to certain modular forms in characteristic zero, and (2) the cohomology of certain spaces in homotopy theory in characteristic p. The torsion is given in terms of the structure of a "p-divided power algebra".

The work is an extension of the work in [CCS13] as well as extensions of a classical computation of Shimura to integral coefficients. The results here contrast the local coefficients such as that in [Loo96] and [Til10].

1. Introduction

In a previous paper ([CCS13]) we considered the ring $M = \mathbb{Z}[x,y]$ of two variables integral polynomials as an $SL_2(\mathbb{Z})$-module: the action on M is given by extending to the symmetric algebra the natural action over $\mathbb{Z}^2$. Of course, M decomposes as an $SL_2(\mathbb{Z})$-representation into its homogeneous components of degree n: $M = \oplus_{n\geq 0} M_n$. We also considered the short exact sequence

$$1 \longrightarrow \mathbb{Z} \xrightarrow{j} B_3 \xrightarrow{\lambda} SL_2(\mathbb{Z}) \longrightarrow 1 \tag{1}$$

where λ is the natural representation of the braid group B_3 to the mapping class group of a genus 1 surface, taking the two standard generators of B_3 into the automorphisms induced by Dehn twists around one parallel and one meridian respectively. The kernel of λ is given by twice the center of B_3. Therefore, M is also a B_3-module with the induced action. In the above cited paper we completely determined the cohomology of B_3 and of $SL_2(\mathbb{Z})$ with coefficients in the module M. The answer is not at all trivial: the free part of the resulting cohomology is related to the dimension of certain spaces of modular functions, while the p-torsion is expressed in terms of divided powers rings. The intriguing connections of the torsion part with some important topological constructions related to homotopy theory is still to be understood.

It is natural to ask if our methods can be extended to the plethora of well-known subgroups of $SL_2(\mathbb{Z})$. In this paper we answer this question affirmatively for one of the main classes of subgroups of $SL_2(\mathbb{Z})$, the so called *principal congruence subgroups of level* n, $\Gamma(n) \subset SL_2(\mathbb{Z})$. Recall that $\Gamma(n)$ is defined as the kernel of the mod-n reduction map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})$. We extend our

Date: August 13, 2013.
*Partially supported by DARPA.

methods to this case, by computing the cohomology both of $\Gamma(n)$ and of the group $B_{\Gamma(n)} := \lambda^{-1}(\Gamma(n))$, with coefficients in the above defined representations. The case $n = 2$ is particularly significant: $\Gamma(2)$ is the kernel of the map to the symmetric group $S_3 = SL_2(\mathbb{Z}/2\mathbb{Z})$ and $B_{\Gamma(2)} \subset B_3$ is the pure braid group P_3 on three strands.

With respect to [CCS13] the computation of the cohomology becomes easier from the facts that $\Gamma(n)$ is either a free group of finite rank, for $n > 2$, or a product of a free group times $\mathbb{Z}_2$, for $n = 2$. Therefore the cohomology of $\Gamma(n)$ is trivial in dimension higher than one (for $n > 2$). However, the description of the first cohomology group, that is done in terms of a so called *$p-$divided polynomial algebra* described below, is similar to that of $SL_2(\mathbb{Z})$ and is given in the following theorem:

Theorem A (Theorem 2.15)**.** *Let p be a prime number and $m > 1$ an integer. If p is a prime that does not divides m the p-torsion component of $H^1(\Gamma(m); M_n)$ is given by:*

$$H^1(\Gamma(m); M_n)_{(p)} = H^1(SL_2(\mathbb{Z}); M_n)_{(p)} = \Delta_p^+[\mathcal{P}_p, \mathcal{Q}_p]_{\deg=n}$$

where $\mathcal{P}_p$ and $\mathcal{Q}_q$ are elements of degree $\deg \mathcal{P}_p = 2(p+1)$ and $\deg \mathcal{Q}_p = 2p(p-1)$. If p divides m, suppose $p^a \mid m, p^{a+1} \nmid m$. Then we have

$$H^1(\Gamma(m); M_{>0})_{(p)} \simeq \Delta_{p^a}^+[x, y]$$

where x, y are elements of degree 1.

The complete description of the cohomology of the subgroup $B_{\Gamma(n)}$, which has cohomological dimension two, is given by:

Theorem B (Theorem 2.17)**.** *The cohomology of the group $B_{\Gamma(m)}$ with coefficients in the module $M = \mathbb{Z}[x, y]$ is given as follows:*

a) *for $m = 2$ and $n = 0$*

$$H^0(B_{\Gamma(2)}; M_0) = \mathbb{Z},$$
$$H^1(B_{\Gamma(2)}; M_0) = \mathbb{Z}^3$$
$$H^2(B_{\Gamma(2)}; M_0) = \mathbb{Z}^2$$

and all the others cohomology groups are zero;

b) *for $m = 2$ and even $n > 0$ we have*

$$H^0(B_{\Gamma(2)}; M_n) = H^0(\Gamma(2); M_n),$$
$$H^1(B_{\Gamma(2)}; M_n) = H^2(B_{\Gamma(2)}; M_n) = H^1(\Gamma(2); M_n)$$

and all the others cohomology groups are zero;

c) *for $m = 2$ and odd n*

$$H^1(B_{\Gamma(2)}; M_n) = H^1(\Gamma(2); M_n) = M_n \otimes \mathbb{Z}/2\mathbb{Z},$$
$$H^2(B_{\Gamma(2)}; M_n) = H^2(\Gamma(2); M_n) = (M_n \oplus M_n) \otimes \mathbb{Z}/2\mathbb{Z}$$

and all the others cohomology groups are zero;

d) *for any $m > 2$*

$$H^*(B_{\Gamma(m)}; M_n) = H^*(\Gamma(m); M_n) \otimes H^*(\mathbb{Z}; \mathbb{Z}).$$

The work here is an extension of the work in [CCS13] as well as extensions of a classical computation of Shimura to integral coefficients. The results presented in this paper contrast the local coefficients such as that in [Loo96] and [Til10].

2. Principal congruence subgroups

It is well known that the subgroup $\Gamma(n) \subset SL_2(\mathbb{Z})$ is either a finitely generated free group or a product of a finitely generated free group with $\mathbb{Z}/2\mathbb{Z}$ (see [Fra33, Gro50]). This fact follows from the decomposition $PSL_2(\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$, so by the Kurosh subgroup Theorem ([Kur34]) the kernel of the map

$$PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}/n\mathbb{Z})$$

is always free. Hence $\Gamma(2)$ is the product of a free group with $\mathbb{Z}/2\mathbb{Z} = \{I, -I\}$, while for $n > 2$ one gets that $\Gamma(n)$ is free.

We write $B_{\Gamma(n)}$ for the inverse image $\lambda^{-1}(\Gamma(n))$ in B_3 (see (1) in the introduction).

In the following we show how to extend the computations in [CCS13] of the cohomology of $SL_2(\mathbb{Z})$ and of B_3 to that of $\Gamma(n)$ and of $B_{\Gamma(n)}$. A special case (as said in the introduction) is $n = 2$: we have the isomorphism

$$SL_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$$

onto the symmetric group S_3, while

$$B_{\Gamma(2)} \simeq P_3$$

is the pure braid group on three strands.

Recall that the group $SL_2(\mathbb{Z})$ is generated by the elements

$$s_1 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \text{ and } s_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and the action on the module $M = \mathbb{Z}[x, y]$ is given by:

$$s_1 : \begin{cases} x \mapsto x - y \\ y \mapsto y \end{cases} \qquad s_2 : \begin{cases} x \mapsto x \\ y \mapsto x + y. \end{cases}$$

We start with some preliminary results.

Proposition 2.1. *Let $m > 1$ be an integer. Let G be a subgroup of $SL_2(\mathbb{Z})$ containing the elements s_1^b and s_2^c such that b and c are coprimes with m. The restriction of the projection $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z})$ to the subgroup G is a surjective map.*

Proof. Recall that the projection $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z})$ is surjective (see, for example, [CCS13]). As a consequence the proposition is straightforward since b and c are invertible mod m and hence a suitable power of s_1^b (resp. s_2^c) maps to s_1 (resp. s_2) in $SL_2(\mathbb{Z}/m\mathbb{Z})$. □

Proposition 2.2. *If the integer $m > 1$ factorizes as $m = p_1^{a_1} \cdots p_k^{a_k}$ then*

$$SL_2(\mathbb{Z}/m\mathbb{Z}) \simeq SL_2(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times SL_2(\mathbb{Z}/p_k^{a_k}\mathbb{Z}). \tag{2}$$

Proof. The result is an easy consequence of the Chinese Remainder Theorem (see also [Han06]). □

Proposition 2.3. *Let m be a positive integer and let p be a prime that does not divide m. For each non-negative integer a and for any integer n we have*

$$H^0(\Gamma(m); M_n \otimes \mathbb{Z}/p^a\mathbb{Z}) = H^0(SL_2(\mathbb{Z}); M_n \otimes \mathbb{Z}/p^a\mathbb{Z}).$$

Proof. The result follows from Proposition 2.1 applied to $s_1^m, s_2^m \in \Gamma(m)$, since

$$H^0(\Gamma(m); M_n \otimes \mathbb{Z}/p^a\mathbb{Z}) = (\mathbb{Z}/p^a\mathbb{Z}[x,y])^{\Gamma(m)} = (\mathbb{Z}/p^a\mathbb{Z}[x,y])^{SL_2(\mathbb{Z})} = H^0(SL_2(\mathbb{Z}); M_n \otimes \mathbb{Z}/p^a\mathbb{Z})$$ □

We need to recall the following result:

Proposition 2.4 ([Ste87], Theorem H and following remarks)**.** *Let p be a prime number and let a, b be positive integers, $a \leq b$. The module $H^0(\Gamma(p^a); M \otimes \mathbb{Z}/p^b\mathbb{Z})$ is generated by polynomials of the form*

$$cP(x^d, y^d)$$

where c is a positive integer such that the power p^{b-a} divides the product cd.

We will need a slightly generalized version of Proposition 2.4:

Proposition 2.5. *Let p be a prime number and let a, b be positive integers, $a \leq b$. Let m be a positive integer and suppose $p^a \mid m$ and $p^{a+1} \nmid m$. The module $H^0(\Gamma(m); M \otimes \mathbb{Z}/p^b\mathbb{Z})$ is generated by polynomials of the form*

$$cP(x^d, y^d)$$

where c is a positive integer such that the power p^{b-a} divides the product cd.

Proof. Our aim is to prove that

$$H^0(\Gamma(m); M \otimes \mathbb{Z}/p^b\mathbb{Z}) = H^0(\Gamma(p^a); M \otimes \mathbb{Z}/p^b\mathbb{Z})$$

so that we can reduce our result to the previous proposition. The equality above is equivalent to

$$(M \otimes \mathbb{Z}/p^b\mathbb{Z})^{\Gamma(m)} = (M \otimes \mathbb{Z}/p^b\mathbb{Z})^{\Gamma(p^a)}.$$

Since the action of $\Gamma(m)$ and $\Gamma(p^a)$ on the module $M \otimes \mathbb{Z}/p^b\mathbb{Z}$ factors through the action of the group $SL_2(\mathbb{Z}/p^b\mathbb{Z})$ we need to show that the groups $\Gamma(m)$ and $\Gamma(p^a)$ have the same image with respect to the projection $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/p^b\mathbb{Z})$.

Let us consider the following commutative diagram:

$$\begin{array}{ccccc} \Gamma(p^a) & \hookrightarrow & SL_2(\mathbb{Z}) & \twoheadrightarrow & SL_2(\mathbb{Z}/p^b\mathbb{Z}) \\ \uparrow & & \uparrow \simeq & & \uparrow \\ \Gamma(m) & \hookrightarrow & SL_2(\mathbb{Z}) & \twoheadrightarrow & SL_2(\mathbb{Z}/p^{b-a}m\mathbb{Z}). \end{array}$$

Since we assume $a < b$, the projections $\Gamma(p^a) \to SL_2(\mathbb{Z}/p^b\mathbb{Z})$ and $\Gamma(m) \to SL_2(\mathbb{Z}/p^{b-a}m\mathbb{Z})$ factor through the quotients

$$\begin{array}{ccc} \Gamma(p^a) & \longrightarrow & SL_2(\mathbb{Z}/p^b\mathbb{Z}) \\ & \searrow \quad \nearrow & \\ & \Gamma(p^a)/\Gamma(p^b) & \end{array} \quad \text{and} \quad \begin{array}{ccc} \Gamma(m) & \longrightarrow & SL_2(\mathbb{Z}/p^{b-a}m\mathbb{Z}) \\ & \searrow \quad \nearrow & \\ & \Gamma(m)/\Gamma(p^{b-a}m) & \end{array}$$

and finally, since $\Gamma(p^b) \cap \Gamma(m) = \Gamma(p^{b-a}m)$, the inclusion $\Gamma(m) \hookrightarrow \Gamma(p^a)$ induces the inclusion

$$\Gamma(m)/\Gamma(p^{b-a}m) \hookrightarrow \Gamma(p^a)/\Gamma(p^b).$$

The result follows since

$$|\,\Gamma(m)/\Gamma(p^{b-a}m)\,| = \frac{|\,SL_2(\mathbb{Z}/p^{b-a}m\mathbb{Z})\,|}{|\,SL_2(\mathbb{Z}/m\mathbb{Z})\,|} = \frac{|\,SL_2(\mathbb{Z}/p^b\mathbb{Z})\,|}{|\,SL_2\mathbb{Z}/p^a\mathbb{Z}\,|} = |\,\Gamma(p^a)/\Gamma(p^b)\,|$$

(the equality in the middle is a consequence of Proposition 2.2) and hence we have the following commutative diagram

$$\begin{array}{ccc} \Gamma(p^a)/\Gamma(p^b) & \longrightarrow & SL_2(\mathbb{Z}/p^b\mathbb{Z}) \\ \uparrow \simeq & & \uparrow \\ \Gamma(m)/\Gamma(p^{b-a}m) & \longrightarrow & SL_2(\mathbb{Z}/p^{b-a}m\mathbb{Z}) \end{array}$$

that implies that the groups $\Gamma(m)$ and $\Gamma(p^a)$ have the same image in $SL_2(\mathbb{Z}/p^b\mathbb{Z})$. □

Let us consider the case $\Gamma(2)$. The group $\Gamma(2)$ is the direct product of a free group F_2 generated by the elements

$$s_1^2 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \text{ and } s_2^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

and the cyclic group $\mathbb{Z}/2\mathbb{Z}$ generated by

$$w_2 = (s_1 s_2 s_2)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proposition 2.6. *The map $\pi_2 : \Gamma(2) \to \mathbb{Z}/2\mathbb{Z}$ defined by*

$$\Gamma(2) \ni A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \overset{\pi_2}{\mapsto} a_{11} \in \mathbb{Z}/4\mathbb{Z}^* \simeq \mathbb{Z}/2\mathbb{Z}.$$

is the projection homomorphism onto the second component of the decomposition $\Gamma(2) = F_2 \times \mathbb{Z}/2\mathbb{Z}$ described above.

Proof. Since the matrix $A = (a_{ij})$ is in $\Gamma(2)$ we have that a_{11} is invertible $\mod 4$. We verify that the map defined in the proposition is a group homomorphism: in fact given $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ two elements in $\Gamma(2)$ we have that $a_{11}b_{11} \equiv a_{11}b_{11} + a_{12}b_{21} \mod 4$ and hence $\pi_2(A)\pi_2(B) = \pi_2(A \cdot B)$. Finally it is easy to verify that $F_2 = \ker \pi_2$. □

We obtain a resolution for a $\Gamma(2)$-module N as in the following diagram taking the product of the standard periodic resolution for $\mathbb{Z}/2\mathbb{Z}$ (horizontal lines) and the minimal resolution for F_2 (vertical lines):

$$\begin{array}{ccccccccc} & & N\oplus N & \xrightarrow{w_2-I} & N\oplus N & \xrightarrow{w_2+I} & N\oplus N & \xrightarrow{w_2-I} & N\oplus N \xrightarrow{w_2+I}\cdots \\ & & \uparrow{\scriptstyle (s_1^2-I,s_2^2-I)} & & \uparrow{\scriptstyle (s_1^2-I,s_2^2-I)} & & \uparrow{\scriptstyle (s_1^2-I,s_2^2-I)} & & \uparrow{\scriptstyle (s_1^2-I,s_2^2-I)} \\ & & N & \xrightarrow[w_2-I]{} & N & \xrightarrow[w_2+I]{} & N & \xrightarrow[w_2-I]{} & N \xrightarrow[w_2+I]{}\cdots \end{array} \tag{3}$$

Recall that the generator w_2 acts trivially on even degree polynomials, while it acts as (-1)-multiplication on odd degree polynomials. Applying this observation to the previous diagram we get the following result:

Proposition 2.7. *Let F_2 be the subgroup of $SL_2(\mathbb{Z})$ freely generated by s_1^2, s_2^2. The following isomorphisms hold. For even n:*

$$H^0(\Gamma(2); M_n) = H^0(F_2; M_n) = \begin{cases} \mathbb{Z} \text{ if } n = 0; \\ 0 \text{ if } n > 0; \end{cases}$$

$$H^1(\Gamma(2); M_n) = H^1(F_2; M_n),$$

and for $i > 0$

$$H^{2i}(\Gamma(2); M_n) = H^0(F_2; M_n \otimes \mathbb{Z}/2\mathbb{Z}) = M_n \otimes \mathbb{Z}/2\mathbb{Z},$$

$$H^{2i+1}(\Gamma(2); M_n) = H^1(F_2; M_n) \otimes \mathbb{Z}/2\mathbb{Z}.$$

For odd n

$$H^0(\Gamma(2); M_n) = H^0(F_2; M_n) = 0,$$

and for $i > 0$

$$H^{2i-1}(\Gamma(2); M_n) = H^0(F_2; M_n \otimes \mathbb{Z}/2\mathbb{Z}) = M_n \otimes \mathbb{Z}/2\mathbb{Z},$$

$$H^{2i}(\Gamma(2); M_n) = H^1(F_2; M_n) \otimes \mathbb{Z}/2\mathbb{Z} = H^1(F_2; M_n \otimes \mathbb{Z}/2\mathbb{Z}).$$

Moreover for any n we have

$$H^1(F_2; M_n \otimes \mathbb{Z}/2\mathbb{Z}) = (M_n \oplus M_n) \otimes \mathbb{Z}/2\mathbb{Z}.$$

Proof. The proposition follows from an analysis of the resolution of $\Gamma(2)$ given in (3). The last statement about the cohomology of F_2 follows since the action of the group F_2 on the module $M \otimes \mathbb{Z}/2\mathbb{Z}$ is trivial. □

Proposition 2.8. *The group $H^0(\Gamma(m); M_n)$ is isomorphic to M_0 for $n = 0$ and is trivial for $n > 0$. Let $p > 2$ be a prime number. The group $H^1(\Gamma(p); M_n \otimes \mathbb{Q})$ has rank $1 + p(p^2-1)/12$ for $n = 0$ and $(n+1)p(p^2-1)/12$ for $n > 0$. For $p = 2$ we have the isomorphism $H^1(\Gamma(2); M_n \otimes \mathbb{Q}) = \mathbb{Q}^2$, concentrated in degree 0.*

Proof. The first statement is trivial, since we have that $s_1^m, s_2^m \in \Gamma(m)$. The second statement follows from a result of Frasch ([Fra33]): for $p > 2$ the group $\Gamma(p)$ is free on $N(p) = 1 + p(p^2 - 1)/12$ generators. We apply this result using the minimal resolution of the free group $\Gamma(p)$. The computation of the rank follows since the submodule of invariants in M_n is trivial for $n > 0$ and hence the differential $\delta_0 : M_n \to M_n^{N(p)}$ is injective. The case $p = 2$ can be easily checked separately by using the formulas from Proposition 2.7. □

We can compute the rank of $\Gamma(m)$ as a free group for any m ($m > 2$).

Lemma 2.9. *Let m be an integer, $m > 2$. Suppose that m is not prime and let p be a prime that divides m. Then we have that $\Gamma(m) \subset \Gamma(p)$. Let i be the index*

$$i = [\Gamma(p) : \Gamma(m)] = |\, SL_2(\mathbb{Z}/m\mathbb{Z})\,| \;/\; |\, SL_2(\mathbb{Z}/p\mathbb{Z})\,| \,.$$

If $p \neq 2$ the group $\Gamma(p)$ is free and the Schreier index formula ([Sch27]*) gives us that $\Gamma(m)$ is a group of rank*

$$r = \mathrm{rk}\Gamma(m) = i(\mathrm{rk}\Gamma(p) - 1) + 1.$$

In the case $p = 2$ the group $\Gamma(2)$ is not free but it contains a rank-2 free subgroup F_2 of index 2.

Proof. If $m \equiv 0 \mod 4$ then $\pi_2(\Gamma(m)) = 1$ (see 2.6) so $\Gamma(m) \subset F_2$. Hence Schreier formula become:

$$r = \mathrm{rk}\Gamma(m) = i/2 + 1.$$

Now let us consider the case $m \equiv 2 \mod 4$ we claim that $\Gamma(m)$ is not contained in F_2. In fact we can consider the element $U_m := \begin{pmatrix} m+1 & -m \\ m & -m+1 \end{pmatrix} \in \Gamma(m)$ and we can see that $\pi_2(U_m) = -1 \mod 4$. In order to determine the rank of $\Gamma(m)$ one can consider the inclusion $\Gamma(m) \cap F_2 \subset F_2$, of index $i = [\Gamma(2) : \Gamma(m)]$ and the inclusion $\Gamma(m) \cap F_2 \subset \Gamma(m)$, of index 2. From the first inclusion Schreier formula tells us that $\Gamma(m) \cap F_2$ is a free group of rank $i + 1$. From the second inclusion Schreier formula gives

$$\mathrm{rk}(\Gamma(m) \cap F_2) = 2(\mathrm{rk}\Gamma(m) - 1) + 1$$

and then $\mathrm{rk}\Gamma(m) = i/2 + 1$.

As a consequence we can use the same argument of Proposition 2.8 and compute the dimension of $H^1(\Gamma(m); M_n \otimes \mathbb{Q})$ for any m using the following formulas:

$$|\, SL_2(\mathbb{Z}/p\mathbb{Z})\,| = (p+1)(p-1)p$$

and (see for example [Han06])

$$|\, SL_2(\mathbb{Z}/p^a\mathbb{Z})\,| = p^{(a-1)3}(p+1)p(p-1).$$

□

From Proposition 2.2 and Lemma 2.9 we have the following generalization of Proposition 2.8:

Proposition 2.10. *Let $m > 2$ be an integer that factors as $m = p_1^{a_1} \cdots p_k^{a_k}$. The cardinality of $SL_2(\mathbb{Z}/m\mathbb{Z})$ is given by*

$$d = \prod_i p_i^{(a_i-1)3} p_i(p_i^2 - 1)$$

and if we define $i = \frac{d}{p_1(p_1^2-1)}$ then $\Gamma(m)$ is a free group of rank

$$r = \begin{cases} i/2 + 1 & \text{if } p_1 = 2 \\ i(p_1(p_1^2 - 1) - 1) + 1 & \text{if } p_1 > 2 \end{cases}$$

The rank of the group $H^1(\Gamma(m); M_n \otimes \mathbb{Q})$ is r, for $n = 0$ and $(r-1)(n+1)$ for $n > 0$. □

Remark 2.11. In the factorization of m used in Proposition 2.8 the primes p_i's need not be ordered, so any prime factor of m can be used in the formula to compute the rank of $\Gamma(m)$.

We now consider the torsion part of the cohomology. We need to recall the notion of *divided polynomial algebra*, as defined in [CCS13]. We present a slightly more general definition.

Let $\mathbb{Q}[x]$ be the ring of rational polynomials in one variable. One defines the subring

$$\Delta[x] := \Delta_{\mathbb{Z}}[x] \subset \mathbb{Q}[x]$$

as the subset generated, as a $\mathbb{Z}$-submodule, by the elements $x_n := \frac{x^n}{n!}$ for $n \in \mathbb{N}$.

Notational remark. The most frequent notation for this ring uses the letter Γ instead of Δ; for obvious reasons, we decided to change it to avoid confusion with the principal congruence subgroups.

It follows from

$$x_i x_j = \binom{i+j}{i} x_{i+j} \tag{4}$$

that $\Delta[x]$ is a sub-algebra of $\mathbb{Q}[x]$, usually known as the *divided polynomial algebra* over $\mathbb{Z}$. One can define $\Delta_R[x] := \Delta[x] \otimes R$ over any ring R.

Let p be a prime number and p^a a power of p. Consider the $p-$adic valuation $v := v_p : \mathbb{N}\backslash\{0\} \to \mathbb{N}$ such that $p^{v(n)}$ is the maximum power of p dividing n.

Define the ideal I_{p^a} of $\Delta[x]$ as

$$I_{p^a} := (p^{v(i)+a}\, x_i, \quad i \geq 1)$$

and call the quotient

$$\Delta_{p^a}[x] := \Delta[x]/I_{p^a}$$

the *p^a-local divided polynomial algebra.*

The following two propositions were proven in [CCS13] for $a = 1$. Exactly the same proof works for any $a \geq 1$.

Proposition 2.12. *The ring $\Delta_{p^a}[x]$ is naturally isomorphic to the quotient*

$$\mathbb{Z}[\xi_1, \xi_p, \xi_{p^2}, \xi_{p^3}, \ldots]/J_{p^a}$$

where J_{p^a} is the ideal generated by the polynomials

$$p^a\xi_1\ , \quad \xi_{p^i}^p - p\xi_{p^{i+1}}\ (i \geq 1).$$

The element ξ_{p^i} corresponds to the generator $x_{p^i} \in \Delta_{p^a}[x],\ i \geq 0$. □

Proposition 2.13. *Let $\mathbb{Z}_{(p)}$ be the local ring obtained by inverting numbers prime to p and let $\Delta_{\mathbb{Z}_{(p)}}[x]$ be the divided polynomial algebra over $\mathbb{Z}_{(p)}$. One has an isomorphism:*

$$\Delta_{p^a}[x] \ \cong\ \Delta_{\mathbb{Z}_{(p)}}[x]/(p^a x).$$

□

Notice that if $\Delta[x]$ is graded with $\deg x = k$, then $\mathbb{Z}[\xi_1, \xi_p, \xi_{p^2}, \ldots]/J_{p^a}$ is graded with $\deg \xi_{p^i} = kp^i$.

A multi-variable divided polynomial algebra is defined as

$$\Delta[x, x', x'', \ldots] := \Delta[x] \otimes_{\mathbb{Z}} \Delta[x'] \otimes_{\mathbb{Z}} \Delta[x''] \otimes_{\mathbb{Z}} \cdots$$

with the ring structure induced as subring of $\mathbb{Q}[x, x', x'', \ldots]$. We have also

$$\Delta_{p^a}[x, x', x'', \ldots] := \Delta_{p^a}[x] \otimes_{\mathbb{Z}} \Delta_{p^a}[x'] \otimes_{\mathbb{Z}} \Delta_{p^a}[x''] \otimes_{\mathbb{Z}} \cdots .$$

We also define the submodule

$$\Delta^+_{p^a}[x, x', x'', \ldots] := \Delta_{p^a}[x, x', x'', \ldots]_{\deg > 0}.$$

Given a finitely generated $\mathbb{Z}$-module A we define FA, the *free part* of A, as a maximal free $\mathbb{Z}-$submodule of A. The module A can be splitted as $A = FA \oplus T$ where T is the submodule of all torsion elements of A. Although the splitting is not canonical and module FA is not well defined, still the isomorphism class of FA and its rank are well defined. We recall from [CCS13] the following description of the first cohomology group of $SL_2(\mathbb{Z})$:

Theorem 2.14 ([CCS13] Theorem 3.7)**.** *Let $M = \oplus_{n\geq 0}\ M_n \simeq H^*((\mathbb{CP}^\infty)^2; \mathbb{Z})$ be the $SL_2(\mathbb{Z})$-module already defined. Then the cohomology $H^1(SL_2(\mathbb{Z}); M_n)$ is given as follows:*

(1) *the p-torsion component is given by*

$$H^1(SL_2(\mathbb{Z}); M_n)_{(p)} = \Delta^+_p[\mathcal{P}_p, \mathcal{Q}_p]_{\deg = n}$$

where we fix gradings $\deg \mathcal{P}_p = 2(p+1)$ and $\deg \mathcal{Q}_p = 2p(p-1)$;

(2) *the free part is*

$$FH^1(SL_2(\mathbb{Z}); M_n) = \mathbb{Z}^{f_n}$$

for $n > 0$ where the rank f_n is given by the Poincaré series

$$P^1_{SL_2(\mathbb{Z}),0}(t) = \sum_{n=0}^{\infty} f_n t^n = \frac{t^4(1 + t^4 - t^{12} + t^{16})}{(1 - t^8)(1 - t^{12})}.$$

We come back now to the torsion part of the cohomology of the principal congruence subgroups $\Gamma(n)$.

By means of the Universal Coefficients Theorem we can compute the p-torsion part of the first cohomology group $H^1(\Gamma(m); M_n)$ by comparing it with the group $H^0(\Gamma(m); M_n \otimes \mathbb{Z}/p^a\mathbb{Z})$. This is described in Proposition 2.3 in the case of a prime p that does not divide m and in Proposition 2.5 in the case that p divides m.

Theorem 2.15. *Let p be a prime number and $m > 1$ an integer. If p is a prime that does not divides m the p-torsion component of $H^1(\Gamma(m); M_n)$ is given by:*

$$H^1(\Gamma(m); M_n)_{(p)} = H^1(SL_2(\mathbb{Z}); M_n)_{(p)} = \Delta_p^+[\mathcal{P}_p, \mathcal{Q}_p]_{\deg=n}$$

where $\mathcal{P}_p$ and $\mathcal{Q}_q$ are elements of degree $\deg \mathcal{P}_p = 2(p+1)$ and $\deg \mathcal{Q}_p = 2p(p-1)$. If p divides m, suppose $p^a \mid m, p^{a+1} \nmid m$. Then we have

$$H^1(\Gamma(m); M_{>0})_{(p)} \simeq \Delta_{p^a}^+[x, y]$$

where x, y are elements of degree 1. □

Remark 2.16. For $m > 2$, since $\Gamma(m)$ is free and hence it has homological dimension 1, a complete description of the cohomology of $\Gamma(m)$ comes directly from Theorem 2.15. For $m = 2$ the description of the cohomology of $\Gamma(m)$ follows from Theorem 2.15 and Proposition 2.7.

Now we focus on the description of the cohomology of the groups $B_{\Gamma(m)}$ defined in the introduction.

The Serre spectral sequence for the extension $\mathbb{Z} \to B_{\Gamma(2)} \to \Gamma(2)$ is concentrated on the first two lines and the E_2-term is the following:

$$\begin{array}{|llll|} \hline H^0(\Gamma(2), M) & H^1(\Gamma(2), M) & H^2(\Gamma(2), M) & \cdots \\ & \searrow^{d_2} & \searrow^{d_2} & \\ H^0(\Gamma(2), M) & H^1(\Gamma(2), M) & H^2(\Gamma(2), M) & \cdots \\ \hline \end{array}$$

hence, for n even we get:

$$\begin{array}{|llll|} \hline H^0(F_2, M_n) & H^1(F_2, M_n) & H^0(F_2, M_n \otimes \mathbb{Z}/2\mathbb{Z}) & H^1(F_2, M_n) \otimes \mathbb{Z}/2\mathbb{Z} \quad \cdots \\ & \searrow^{d_2} & \searrow^{d_2} & \\ H^0(F_2, M_n) & H^1(F_2, M_n) & H^0(F_2, M_n \otimes \mathbb{Z}/2\mathbb{Z}) & H^1(F_2, M_n) \otimes \mathbb{Z}/2\mathbb{Z} \quad \cdots \\ \hline \end{array}$$

and for n odd:

$$\begin{array}{|llll|} \hline 0 & H^0(F_2, M_n \otimes \mathbb{Z}/2\mathbb{Z}) & H^1(F_2, M_n) \otimes \mathbb{Z}/2\mathbb{Z} & H^0(F_2, M_n \otimes \mathbb{Z}/2\mathbb{Z}) \quad \cdots \\ & & \searrow^{d_2} & \\ 0 & H^0(F_2, M_n \otimes \mathbb{Z}/2\mathbb{Z}) & H^1(F_2, M_n) \otimes \mathbb{Z}/2\mathbb{Z} & H^0(F_2, M_n \otimes \mathbb{Z}/2\mathbb{Z}) \quad \cdots \\ \hline \end{array}$$

Recall that the group $B_{\Gamma(2)} = P_3$ has homological dimension 2 and hence the spectral sequence above converges to $E_\infty^{i,j} = 0$ for $i + j > 2$.

For n even we can compute the first differential $d_2^{0,1} : E_2^{0,1} \to E_2^{2,0}$ comparing the spectral sequence above with the spectral sequence for the extension $\mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ associated to the subgroup $\mathbb{Z}/2\mathbb{Z} \subset \Gamma(2) = F_2 \times \mathbb{Z}/2\mathbb{Z}$. It follows that the differential $d_2^{0,1}$ is the map

$$M_0^{\Gamma(2)} \to (M_0 \otimes \mathbb{Z}/2\mathbb{Z})^{\Gamma(2)}$$

induced by the projection map $M_0 \to M_0 \otimes \mathbb{Z}/2\mathbb{Z}$. Hence $\mathbb{Z} \simeq \ker d_2^{0,1} = 2\mathbb{Z} \subset M_0 = \mathbb{Z}$ and $\mathrm{coker} d_2^{0,1} = M_{>0} \otimes \mathbb{Z}/2\mathbb{Z}$. The differential $d_2^{1,1} : E_2^{1,1} \to E_2^{3,0}$ is surjective. All the other maps $d_2 : E_2^{k,1} \to E_2^{k+2,0}$ are isomorphisms.

For odd n the first differential $d_2^{0,1} : E_2^{0,1} \to E_2^{2,0}$ is zero and all the other maps $d_2^{k,1} : E_2^{k,1} \to E_2^{k+2,0}$ are isomorphisms. So $E_\infty^{i,j} = 0$ except for $(i,j) = (1,0)$ or $(i,j) = (2,0)$.

For n even the non-zero E_∞ terms of the spectral sequence with total degree 2 are

$$E_\infty^{1,1} = 2(\Delta_2^+[x,y])_{\deg=n}$$

and

$$E_\infty^{2,0} = M_n \otimes \mathbb{Z}/2\mathbb{Z} = (\Delta_2^+[x,y] \otimes \mathbb{Z}/2\mathbb{Z})_{\deg=n}.$$

We claim that there is an extension such that $H^2(B_{\Gamma(2)}; M) \simeq H^1(\Gamma(2); M)$. This can be proved using methods similar to those used in [CCS13]. We sketch here the main ideas of the proof. We can consider the spectral sequence $\overline{E}$ for $\mathbb{Z} \to B_{\Gamma(2)} \to \Gamma(2)$ with coefficients in the module $M \otimes \mathbb{Z}/2^k\mathbb{Z}$ for any k. Let $\mathbb{Z}/2^i\mathbb{Z}$ be a module that appears as a direct summand in $H^1(F_2, M_n) = E_2^{1,1}$.

If $k < i$ then by Universal Coefficients Theorem the module $\mathbb{Z}/2^i\mathbb{Z}$ determines a module $\mathbb{Z}/2^k\mathbb{Z}$ that is a direct summand in $H^0(F_2, M_n \otimes \mathbb{Z}/2^k\mathbb{Z}) = \overline{E}_2^{0,1}$; moreover the differential $\overline{d}_2$ restricted to $\mathbb{Z}/2^k\mathbb{Z}$ is non trivial, as one can see comparing the spectral sequence $\{\overline{E}_r\}$ with the one associated to the extension $\mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

If $k \geq i$ then by Universal Coefficients Theorem the module $\mathbb{Z}/2^i\mathbb{Z}$ determines a module $\mathbb{Z}/2^i\mathbb{Z}$ that is a direct summand in $H^0(F_2, M_n \otimes \mathbb{Z}/2^k\mathbb{Z}) = \overline{E}_2^{0,1}$; the study of the Bockstein map β_k for the extension $0 \to \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/2^{2k}\mathbb{Z} \to \mathbb{Z}/2^k\mathbb{Z} \to 0$ shows that the differential $\overline{d}_2$ restricted to $\mathbb{Z}/2^k\mathbb{Z}$ is non-trivial and the image $\overline{d}_2(\mathbb{Z}/2^k\mathbb{Z})$ is a direct summand of $\overline{E}_2^{2,0}$ isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

This means that the summand $\mathbb{Z}/2^i\mathbb{Z}$ in $E_2^{1,1}$ give a contribution to the cardinality of $|\oplus_{i+j=2}\overline{E}_\infty^{i,j}| = |H^2(B_{\Gamma(2)}; M \otimes \mathbb{Z}/2^k\mathbb{Z})|$ corresponding to a factor 2^{k-1} for $k < i$ and to a factor 2^{i-1} for $k \geq i$. It follows, by an argument similar to that used in [CCS13], section 7, that the term $\mathbb{Z}/2^i\mathbb{Z}$ in $H^1(F_2, M_n) = E_2^{1,1}$ corresponds to a term $\mathbb{Z}/2^{i-1}\mathbb{Z}$ in $E_\infty^{1,1}$ and there is a summand $\mathbb{Z}/2\mathbb{Z}$ in $E_\infty^{2,0}$ which produce a non-trivial extension

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2^i\mathbb{Z} \to \mathbb{Z}/2^{i-1}\mathbb{Z} \to 0$$

in the exact sequence

$$0 \to E_\infty^{2,0} \to H^2(B_{\Gamma(2)}; M) \to E_\infty^{1,1} \to 0.$$

Hence there is a direct summand $\mathbb{Z}/2^i\mathbb{Z}$ in $H^2(B_{\Gamma(2)}; M)$ associated to the direct summand $\mathbb{Z}/2^i\mathbb{Z} \subset H^1(F_2, M_n)$.

For $m \neq 2$, as we already said, the group $\Gamma(m)$ is free. Hence its cohomology is trivial in dimension bigger than 1 and it follows that the spectral sequence for the extension $\mathbb{Z} \to B_{\Gamma(m)} \to \Gamma(m)$ collapses at the E_2-term. There is no non-trivial extension involved in the E_∞-term, since the cohomology group $H^*(\Gamma(m); M_0)$ is torsion free and for $n > 0$ the cohomology $H^*(\Gamma(m); M_n)$ is concentrated in dimension 1.

Hence we can describe the cohomology of $B_{\Gamma(m)}$ as follows:

Theorem 2.17. *The cohomology of the group $B_{\Gamma(m)}$ with coefficients in the module $M = \mathbb{Z}[x, y]$ is given as follows:*

a) *for $m = 2$ and $n = 0$*

$$H^0(B_{\Gamma(2)}; M_0) = \mathbb{Z},$$
$$H^1(B_{\Gamma(2)}; M_0) = \mathbb{Z}^3$$
$$H^2(B_{\Gamma(2)}; M_0) = \mathbb{Z}^2$$

and all the others cohomology groups are zero;

b) *for $m = 2$ and even $n > 0$ we have*

$$H^0(B_{\Gamma(2)}; M_n) = H^0(\Gamma(2); M_n),$$
$$H^1(B_{\Gamma(2)}; M_n) = H^2(B_{\Gamma(2)}; M_n) = H^1(\Gamma(2); M_n)$$

and all the others cohomology groups are zero;

c) *for $m = 2$ and odd n*

$$H^1(B_{\Gamma(2)}; M_n) = H^1(\Gamma(2); M_n) = M_n \otimes \mathbb{Z}/2\mathbb{Z},$$
$$H^2(B_{\Gamma(2)}; M_n) = H^2(\Gamma(2); M_n) = (M_n \oplus M_n) \otimes \mathbb{Z}/2\mathbb{Z}$$

and all the others cohomology groups are zero;

d) *for any $m > 2$*

$$H^*(B_{\Gamma(m)}; M_n) = H^*(\Gamma(m); M_n) \otimes H^*(\mathbb{Z}; \mathbb{Z}).$$

□

References

[CCS13] Filippo Callegaro, Frederick R. Cohen, and Mario Salvetti, *The cohomology of the braid group B_3 and of $SL_2(\mathbb{Z})$ with coefficients in a geometric representation*, Q. J. Math. (2013), 1–43, published online June 12, 2013.

[Fra33] Hermann Frasch, *Die Erzeugenden der Hauptkongruenzgruppen für Primzahlstufen*, Math. Ann. **108** (1933), no. 1, 229–252.

[Gro50] Emil Grosswald, *On the structure of some subgroups of the modular group*, Amer. J. Math. **72** (1950), 809–834.

[Han06] Juncheol Han, *The general linear group over a ring*, Bull. Korean Math. Soc. **43** (2006), no. 3, 619–626.

[Kur34] A. G. Kurosh, *Die untergruppen der freien produkte von beliebigen gruppen*, Math. Ann. **109** (1934), no. 1, 647–660.

[Loo96] Eduard Looijenga, *Stable cohomology of the mapping class group with symplectic coefficients and of the universal Abel-Jacobi map*, J. Algebraic Geom. **5** (1996), no. 1, 135–150.

[Sch27] O. Schreier, *Die Untergruppen der freien Gruppen.*, Abhandlungen Hamburg **5** (1927), 161–183 (German).

[Ste87] Robert Steinberg, *On Dickson's theorem on invariants*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **34** (1987), no. 3, 699–707.

[Til10] Ulrike Tillmann, *The representation of the mapping class group of a surface on its fundamental group in stable homology*, Q. J. Math. **61** (2010), no. 3, 373–380.

Scuola Normale Superiore, Pisa, Italy
E-mail address: f.callegaro@sns.it

Department of Mathematics, University of Rochester, Rochester NY 14627, USA
E-mail address: cohf@math.rochester.edu

Department of Mathematics, University of Pisa, Pisa Italy
E-mail address: salvetti@dm.unipi.it