A combinatorial interpretation of the probabilities of p-groups in the Cohen-Lenstra measure

Johannes Lengler

July 31, 2007

Abstract

In this paper, I will introduce a link between the volume of a finite abelian p-group in the Cohen-Lenstra measure and partitions of a certain type. These partitions will be classified by the output of an algorithm. Furthermore, I will derive a formula (7.2) for the probability of a p-group to have a specific exponent.

1 Introduction

In [2], Cohen and Lenstra introduced a measure on finite abelian p-groups that seems to describe how those groups behave if they are "randomly" generated. This seems to be the case for some important examples. E.g., take for each positive, squarefree n the field $\mathbb{Q}(\sqrt{-n})$. This field has a (finite abelian) class group over $\mathbb{Q}$. We consider the p-part of this group for some prime $p \neq 2$. In this way, we get a sequence of finite abelian p-groups.

A lot of effort has been put into investigating this sequence. It is conjectured (and all computational tests give strong evidence) that it behaves precisely like a randomly generated sequence (w.r.t the Cohen Lenstra measure). If this could be proven, the implications would be overwhelming. For example, the fraction of imaginary quadratic fields with cyclic class group (neglecting the even part, see [2]) would be 97.75...%.

Even more interesting is the case of realquadratic number fields. It is not known whether there are infinitely many such fields with unique prime element factorization. However, the Cohen-Lenstra conjectures predicts that 75.44...% of those groups have this property. (The conjectured distribution is not exactly the Cohen-Lenstra distribution, but can be derived from it, see [2] for details.)

There are similar conjectures for other sequences of finite abelian p-groups. But at the moment, no promising approach to proving such conjectures is known. However, there is a hint that comes out of the measure itself. The total volume of the space of all finite abelian p-groups is (non-normalized; see below for definitions)

$$\sum_{\substack{G \text{ finite} \\ \text{abelian } p\text{-group}}} \text{volume}(\{G\}) \quad = \quad \sum_{n \in \mathbb{N}} \sum_{\substack{\underline{n} \text{ is a par-} \\ \text{tition of } n}} q^n, \tag{1}$$

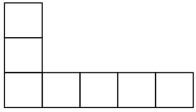
with $q = p^{-1}$.
On the left hand side (as we will see) each summand is a power series with positive coefficients. On the right hand side we have a sum of monomials. So it is natural to suppose that not only the sums are equal, but rather each term on the left hand side corresponds to a selection of terms on the right hand side, in some natural way. In other words, there should be a link between finite abelian p-groups and partitions. (Beyond the obvious one stemming from the elementary divisor theorem.)
This paper presents such a link, alongside giving a new proof of formula (1). One hope is that this connection might help to tackle the conjectures mentioned above. Instead of finding a link between fields $\mathbb{Q}(\sqrt{-n})$ and some mysterious formulas, we only need to find a link between fields and concrete combinatorial objects (namely partitions), which might be easier.
The connection established in this paper also allows to immediately derive a new theorem: Namely, an explicit formula (Theorem 7.1) for the probability of a p-group to have a specific exponent, which is not obvious from the standard formulas concerning the Cohen-Lenstra measure.

2 Preliminaries and Notation

In this paper, I will use the following facts without proof.

- For any prime p, finite abelian p-groups can be indexed by partitions (up to isomorphism, i.e., groups which are isomorphic are treated as the same group). E.g. the group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$ gets identified with $(1, 1, 4)$. Throughout this article, all groups are finite abelian p-groups. For simplicity, I will just refer to those as "p-groups", although this is formally incorrect.

- Partitions can be visualized via Young tableaux, in which each row refers to one term. In this paper, the longest row of a Young tableau is at the bottom, e.g.



,

which corresponds to the partition $(1, 1, 5)$. The total number of boxes corresponds to the number that is partitioned, in the example $7 = 1+1+5$.

- The set of all p-groups can be endowed with a probability measure such that the volume of the one-element set $\{G\}$ is given by $\eta_\infty(p)\frac{1}{|\text{Aut}(G)|}$ (cf. Cohen and Lenstra's original work [2], or [3]).

Here, $\eta_\infty(p) := \prod_{i=1}^\infty (1-p^{-i})$ is a constant scaling factor.
I will refer to this measure as "Cohen-Lenstra measure".

- If
$$G = \prod_{i=1}^{k} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}\text{ , where } 0 < e_1 < e_2 < \ldots < e_k,$$
then
$$|\mathrm{Aut}(G)| = \left(\prod_{i=1}^{k}\left(\prod_{s=1}^{r_i}(1-p^{-s})\right)\right)\left(\prod_{1\le i,j\le k} p^{-\min(e_i,e_j)r_ir_j}\right).$$

The *weight of* G is the formal power series

$$w(G) := \left(\prod_{i=1}^{k}\left(\prod_{s=1}^{r_i}(1-q^{s})^{-1}\right)\right)\left(\prod_{1\le i,j\le k} q^{\min(e_i,e_j)r_ir_j}\right).$$

which, by plugging in $q := p^{-1}$, yields $|\mathrm{Aut}(G)|^{-1}$. This agrees with the notation in the Cohen-Lenstra paper [2], except that Cohen and Lenstra work with evaluated series instead of formal series.
Throughout the article, I will use the following notation:

- $\mathbb{N} = \{0, 1, \ldots\}$.
- $\mathcal{P}$:= Set of all partitions. (Partitions will usually be increasing in this paper, e.g. $(1, 1, 3, 4)$.)
- Partitions will appear in several distinct roles. In particular, as mentioned above, p-groups can be identified with partitions. If partitions are used for indexing p-groups, I will denote the set by $\mathcal{P}_G$, although as a set it is identical with $\mathcal{P}$.
If I use placeholders for partitions, I will usually flag them with an underscore, e.g. $\underline{n} = (1, 1, 11)$.

3 The statement

Cohen and Lenstra have shown ([2]) that

$$\sum_G w(G) \;=\; \prod_{i=1}^{\infty}(1-q^i)^{-1} = \sum_{n\in\mathbb{N}} p(n)q^n = \sum_{n\in\mathbb{N}} \sum_{\substack{\underline{n}\text{ is a par-}\\ \text{tition of } n}} q^n,$$

where $p(n)$ is the number of partitions of n. (As usual, $p(0) = 1$.)
In the introduction, we claimed that the right hand sum should decompose into portions that correspond to the power series on the left hand side. Of course, the existence of some arbitrary decomposition of this kind is trivial, but we want

furthermore that each portion should reflect in a "natural" way the associated group.
The main theorem of this paper will give such a decomposition. I will define an (easy to compute) surjective map Λ that assigns to each partition a p-group, hence decomposes the set of all partitions into a number of subsets labelled by p-groups such that each set has exactly the "correct" size.
Formally speaking, I define a map $\Lambda : \mathcal{P} \to \mathcal{P}_G$ with the following property:

3.1 Theorem. *For a finite p-group G, the mapping Λ defined in sections 4 and 5 can be used to compute $w(G)$ via:*

$$w(G) = \sum_{n \geq 0} a_G(n) q^n,$$

where

$$a_G(n) = \left| \left\{ \Lambda^{-1}(G) \right\} \cap \{ \underline{n} \in \mathcal{P} | \ \underline{n} \text{ is a partition of } n \in \mathbb{N} \} \right| \tag{2}$$

is the number of partitions of n that are mapped onto G.

Hence, Λ has the properties announced in the introduction.
A proof of the theorem will follow in section 6.
Beforehand of course, I have to define the mapping Λ. This will be done in two ways: via Young tableaux and numerically. The next two chapters are devoted to this purpose.
I want to mention that instead of describing Λ directly, there is also another, more intrinsic way indicated by the following commutative diagram.

$$\begin{tikzcd}
\mathcal{P} \arrow[d, "\pi"'] \arrow[dr, "\Lambda"] & \\
\mathcal{P}_{base} \arrow[r, "\cong"] & \mathcal{P}_G
\end{tikzcd} \quad ,$$

where $\mathcal{P}_{base}$ is a subset of $\mathcal{P}$.
From a theoretical point of view, it may be more appropriate to work with π instead of Λ since π has nicer properties. In particular, π is a projection ($\pi^2 = \pi$). However, for computational applications, one needs the composite map Λ. In this paper I will usually work directly with Λ. Details about $\mathcal{P}_{base}$, π and the bijection $\iota : \mathcal{P}_G \overset{\cong}{\longleftrightarrow} \mathcal{P}_{base}$ can be found in section 6.

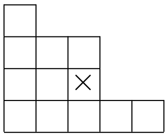
4 Definition of Λ (via Young tableaux)

Let us turn to the definition of the mapping Λ.
The definition in this section is probably harder to read than the one in the next section, but it is closer to the proof of the main theorem. That is why I decided to include this version also. In particular, the example 4.5 will indicate where the object $\mathcal{P}_{base}$ and the numbers a_i from the proof come into play.
First I introduce a new (non-standard) notation:

4.1 Notation.

- In the Young tableau, we denote by $(i, j) \in \mathbb{Z} \times \mathbb{Z}$ the box in the i-th row (counted from the bottom) and the j-th column (counted from the left).

  So in the diagram below, the $(2, 3)$-box is marked:



- Let $(i, j) \in \mathbb{Z} \times \mathbb{Z}$, and let $\lambda \in \mathbb{Z}$. The λ-*successor* $s_\lambda(i, j)$ of (i, j) is the point $(i + 2, j - \lambda) \in \mathbb{Z} \times \mathbb{Z}$. For any $M \subset \mathbb{Z} \times \mathbb{Z}$, let $s_\lambda(M)$ be the image of M under s_λ.

Now Λ can be defined by the following algorithm:

4.2 Algorithm. *Let $\underline{n} \in \mathcal{P}$.*

1. *Let $M_1 \subset \mathbb{N} \times \mathbb{N}$ be the Young tableau of $\underline{n}$. Put $k := 1$.*

2. *Let $Q_k := \{(i, j) \in \mathbb{Z} \times \mathbb{Z} |\ j \geq 1,\ i \geq 2k - 1\}$.*
   Find $\lambda_k \in \mathbb{Z}$ minimal s.t. $s_{\lambda_k}(M_k) \cap Q_k \subset M_k$.

3. *Find the maximum $i_k \in \mathbb{Z}$ s.t. there is a $j \in \mathbb{Z}$ with:*

   - *$(i_k, j) \in M_k$ and*
   - *$s_{\lambda_k - 1}(i_k, j) \in Q_k \setminus M_k$.*

4. *Let $C_k := \{(i, j) |\ i \leq i_k\} \setminus M_k$.*
   Put $Q_{k+1} := \{(i, j) \in \mathbb{Z} \times \mathbb{Z} |\ j \geq 1,\ i \geq 2k + 1\}$.
   Put $M_{k+1} := (M_k \setminus s_{\lambda_k}(C_k)) \cap Q_{k+1}$.
   Increase k by 1.

5. *Repeat step 2-4 until $M_k \cap Q_k$ is empty.*

If the algorithm terminates after k loops, it returns integers $\lambda_1, \ldots, \lambda_k$.
Put $\Lambda(\underline{n}) := (\lambda_k, \lambda_{k-1}, \ldots, \lambda_1) \in \mathcal{P}_G$.

4.3 Remark.

- The algorithm always terminates, so Λ is well-defined.

- The λ_i are sorted: $\lambda_1 \geq \ldots \geq \lambda_k$. Note that we have reversed the order in $\Lambda(\underline{n})$ in order to get a partition.

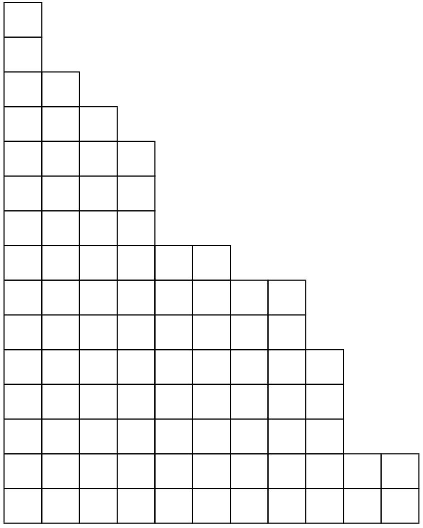
If one wants to write down a rigorous proof, then the following facts are helpful. This remark may be ignored if the reader is willing to believe that the algorithm works as claimed.

4.4 Remark. In the k-th loop, define

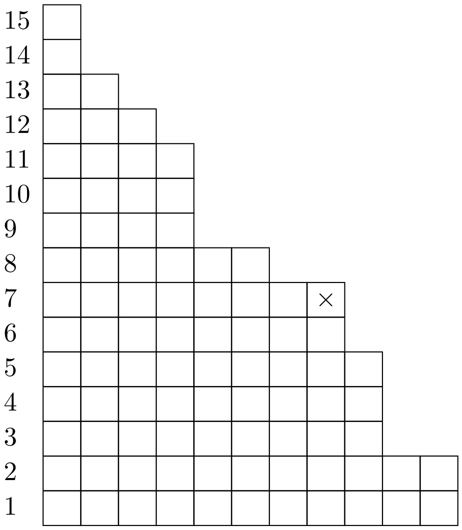
$$a_k := |(M_k)| - |(M_{k+1})| - |\{(i,j) \in M_k|\ i = 2k+1\}| - |\{(i,j) \in M_{k+1}|\ i = 2k+3\}|\,.$$

The a_k quantify the difference between M_k and M_{k+1}, where the two latter terms compensate (roughly speaking) for the two lowest lines, which are cut off from M_{k+1}.
Define further $j_{k,\max} := \max\{j|\ \exists i \text{ s.t. } (i,j) \in M_k\}$. Then in each step after the first we have the invariant $n = |(M_{k+1})| + 2kj_{k,\max} + \left(\sum_{i=1}^{k} \lambda_i(2i-1)\right) + \sum_{i=1}^{k} a_i$.
In particular, after termination the first two terms will vanish, so we get $n = \left(\sum_{i=1}^{k} \lambda_i(2i-1)\right) + \sum_{i=1}^{k} a_i$.

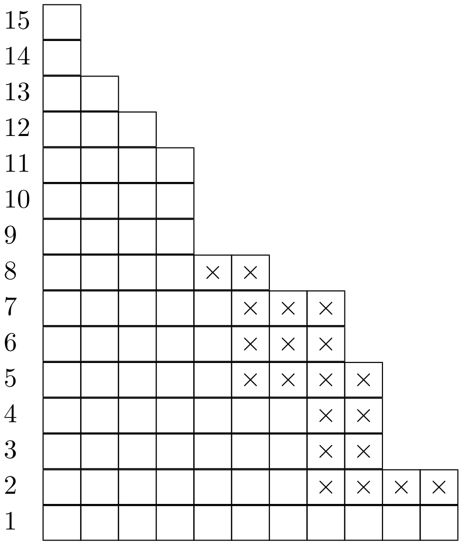
4.5 Example. Let us consider the partition $\underline{n} = (1,1,2,3,4,4,4,6,8,8,9,9,9,11,11)$. Its Young tableau is



In each round, I will give a partition $\underline{n}_k$ that reflects M_k in the following sense: If you draw the Young tableau of $\underline{n}_k$ and intersect it with Q_k (i.e., you forget the $2k-2$ lowest lines), then you get M_k.
In order to save some space, I have only drawn those parts of the Young tableaux that really count, i.e., I have drawn M_k and not the whole of $\underline{n}_k$.
At the beginning, Q_k is the whole first quadrant, so we consider the whole tableau. We find that $\lambda_1 = 4$ and $i_1 = 7$, because the box $(7,8)$ is in M_1, but $s_{4-1} = s_3$ maps $(7,8)$ to $(9,5) \notin M_1$.



The boxes that are marked in the next diagram will be removed according to step 4 of the algorithm. Note that also the two lowest lines will be removed, so it is not really necessary to mark any box in line 2. However, in this way the number of marked boxes is exactly a_1 (cf. remark 4.4). (In general, in the i-th step the number of marked boxes will be a_i.)
If the reader is not interested in the proof, he/she may ignore these data.

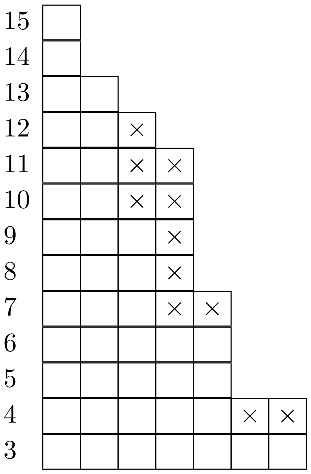


So we get the partition

$$\underline{n}_2 = (1, 1, 2, 3, 4, 4, 4, 4, 5, 5, 5, 7, 7, 7, 11).$$

Now we find that $\lambda_2 = 2$ and $i_2 = 3$, because the box $(12, 3)$ is not mapped into M_2 by $s_{\lambda_2 - 1}$. Remember that, in order to find λ_2 and i_2, we must ignore line 1

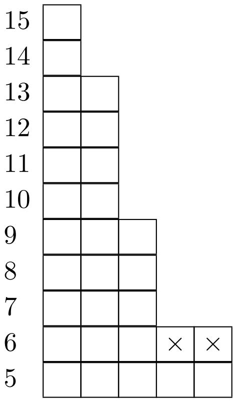
and 2, because they do not belong to Q_2.
Again, we label the boxes which are going to be removed. And again, the reader who is not interested in the proof may ignore line 3 and 4:



We obtain

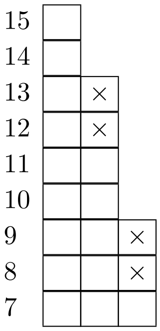
$$\underline{n}_3 = (1, 1, 2, 2, 2, 2, 3, 3, 3, 5, 5, 5, 7, 7, 11),$$

Now we look at M_3 and find $\lambda_3 = 2$ and $i_3 = 6$:



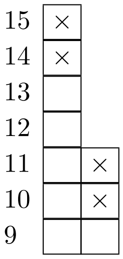
$$\underline{n}_4 = (1, 1, 2, 2, 2, 2, 3, 3, 3, 3, 5, 5, 7, 7, 11).$$

We get $\lambda_4 = 1$, $i_4 = 15$:



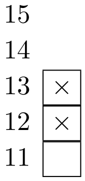
$$\underline{n}_5 = (1,1,1,1,2,2,2,2,3,3,5,5,7,7,11)$$

Next, $\lambda_5 = 1$, $i_5 = 15$.



$$\underline{n}_6 = (0,0,1,1,1,1,2,2,3,3,5,5,7,7,11)$$

Finally, $\lambda_6 = 1$, $i_6 = 13$ and



$$\underline{n}_7 = (0,0,0,0,1,1,2,2,3,3,5,5,7,7,11)$$

M_7 is empty, so the algorithm has terminated and yields:

$$\Lambda(\underline{n}) = (\lambda_6, \lambda_5, \lambda_4, \lambda_3, \lambda_2, \lambda_1) = (1,1,1,2,2,4) \in \mathcal{P}_G.$$

We identify this partition with the group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$.

5 Definition of Λ (numerical)

5.1 Algorithm (numerical). *Let $\underline{n} = (n_1, n_2, \ldots, n_m) \in \mathcal{P}$. The algorithm works as follows:*

1. *We replace $\underline{n}$ by the sequence $\overline{n} = (\overline{n}_1, \overline{n}_2, \dots \overline{n}_m)$, where $\overline{n}_i := n_i - n_{i-2}$, putting $n_0 := n_{-1} := 0$.*

   We put $k := 1$ and $\overline{n}^1 := \overline{n}$.

2. *Let $\lambda_k := \max_l \{\overline{n}_l^k\}$, and let $i_k := \min\{l |\ \overline{n}_l^k = \lambda_k\}$.*

3. *Remove the entries with indices $i_k - 1$, i_k and $i_k + 1$ from $\overline{n}^k$ and replace them by the single new entry $\overline{n}_{i_k-1}^k + \overline{n}_{i_k+1}^k - \overline{n}_{i_k}^k$, thereby getting $\overline{n}^{k+1}$. Increase k by 1.*

   (We might need to use some $\overline{n}_l^k$ that is out of range at this point. In this case, we may add a 0 on the left. The invariants given below guarantee that this cannot happen on the right.)

4. *Repeat step 2 and 3 until $\overline{n}^k$ consists only of zeros.*

The output of the algorithm is $(\lambda_k, \lambda_{k-1}, \lambda_{k-2}, \dots, \lambda_1) \in \mathcal{P}_G$.

5.2 Remark.

- In loop k, all values in the sequence are integers between 0 and λ_{k-1}. In particular, the λ_k are monotonically decreasing.

  Furthermore, it is helpful to note that we have $\overline{n}_{i-1}^k + \overline{n}_{i+1}^k \geq \overline{n}_i^k$ for all i, k.

  These statements can be proved by simple induction.

- This form of the algorithm is much handier and should be used for computations rather than the Young tableau version.

5.3 Example. Let $\underline{n} = (1, 1, 2, 3, 4, 4, 4, 6, 8, 8, 9, 9, 9, 11, 11)$.
I mark the places where something will happen in the next step by bold type. We compute

$$\overline{n}^1 = \overline{n} = (1, 1, 1, 2, 2, 1, 0, \mathbf{2}, \mathbf{4}, \mathbf{2}, 1, 1, 0, 2, 2).$$

Obviously, $\lambda_1 = 4$ and $i_1 = 9$. We have to replace the part 2, 4, 2 by the single entry $2 + 2 - 4 = 0$, getting:

$$\overline{n}^2 = (1, 1, \mathbf{1}, \mathbf{2}, \mathbf{2}, 1, 0, 0, 1, 1, 0, 2, 2).$$

We see that $\lambda_2 = 2$ and $i_2 = 4$. We replace 1, 2, 2 by 1:

$$\overline{n}^3 = (1, 1, 1, 1, 0, 0, 1, 1, \mathbf{0}, \mathbf{2}, \mathbf{2})$$

$\lambda_3 = 2$, $i_3 = 10$, so we must replace 0, 2, 2 by 0:

$$\overline{n}^4 = (\mathbf{1}, \mathbf{1}, 1, 1, 0, 0, 1, 1, 0)$$

Now $\lambda_4 = 1$ and $i_4 = 1$. We fill up one 0 at the left and replace 0, 1, 1 by 0:

$$\overline{n}^5 = (\mathbf{0}, \mathbf{1}, \mathbf{1}, 0, 0, 1, 1, 0)$$

$\lambda_5 = 1$, $i_5 = 2$ and we replace 0, 1, 1 by 0:

$$\overline{n}^6 = (0, \mathbf{0}, \mathbf{1}, \mathbf{1}, 0)$$

Finally, $\lambda_6 = 1$, $i_6 = 3$, and after replacing one last time, we get a sequence of zeros:

$$\overline{n}^7 = (0, 0, 0),$$

so we are done.
The result is $(\lambda_6, \lambda_5, \lambda_4, \lambda_3, \lambda_2, \lambda_1) = (1, 1, 1, 2, 2, 4) \in \mathcal{P}_G$, which by our bijection corresponds to the group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$.

6 Proof of Theorem 3.1

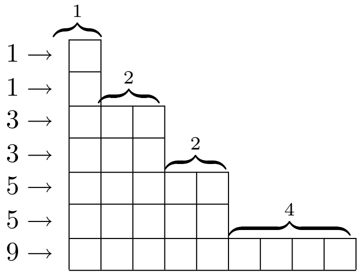
The set $\mathcal{P}_{base} \subset \mathcal{P}$ will under Λ correspond one-to-one with the set $\mathcal{P}_G$ of all partitions. I will define it by constructing an (injective) section $\iota : \mathcal{P}_G \to \mathcal{P}$, i.e., $\Lambda \circ \iota = id_{\mathcal{P}_G}$. Then $\mathcal{P}_{base}$ will be the image under this map.

6.1 Definition. *($\mathcal{P}_{base}$)*
Let G be a (finite abelian) p-group, given by a partition $\underline{n} = (n_1, n_2, \ldots, n_k) \in \mathcal{P}_G$, $0 < n_1 \leq n_2 \leq \ldots \leq n_k$. Then its corresponding element $\iota(\underline{n}) \in \mathcal{P}_{base}$ is defined as the partition

$$\begin{aligned} \underline{n}_{base} := \iota(\underline{n}) \quad := \quad & (n_1, n_1, n_1 + n_2, n_1 + n_2, n_1 + n_2 + n_3, n_1 + n_2 + n_3, \\ & n_1 + n_2 + n_3 + n_4, \ldots, n_1 + n_2 + \ldots + n_k), \end{aligned}$$

where each term appears twice, except for the last one, which appears only once.
$\mathcal{P}_{base} := \iota(\mathcal{P}_G)$

6.2 Example. The group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$ with partition $\underline{n} = (1, 2, 2, 4)$ corresponds to $\underline{n}_{base} = (1, 1, 3, 3, 5, 5, 9)$.
The correspondence can be visualized in the Young Tableau:



A brief look shows that a partition $\underline{m} = (m_1, m_2, \ldots, m_k)$ belongs to $\mathcal{P}_{base}$ iff it satisfies the following conditions:

- k is odd.
- $m_1 = m_2 < m_3 = m_4 < m_5 = \ldots = m_{k-1} < m_k$.
- $0 < m_1 \leq m_3 - m_1 \leq m_5 - m_3 \leq m_7 - m_5 \leq \ldots \leq m_k - m_{k-2}$.

In this case $\underline{m}$ is the image of the partition $(m_1, m_3 - m_1, m_5 - m_3, \ldots, m_k - m_{k-2}) \in \mathcal{P}_G$.
Now we can turn to the

Proof of the main theorem (3.1).
In Remark 4.4, I introduced numbers a_i, which were illustrated in the succeeding example. Recall that if

$$G = \prod_{i=1}^{k} \left(\mathbb{Z}/p^{e_i}\mathbb{Z}\right)^{r_i}, \text{ where } 0 < e_1 < e_2 < \ldots < e_k,$$

then

$$w(G) = \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1-q^s)^{-1} \right) \right) \left(\prod_{1 \le i,j \le k} q^{\min(e_i,e_j) r_i r_j} \right). \qquad (3)$$

Expanding a factor $(1-q^s)^{-1}$ yields $1 + q^s + q^{2s} + q^{3s} + \ldots$.
What is the coefficient of q^n if we multiply out the products? It equals the number of tuples $(b_{i,s})$, each $b_{i,s}$ in $\mathbb{N}$, where i, s run between 1 and k, 1 and r_i, respectively, and such that

$$\sum_{i,s} s b_{i,s} + \sum_{i,j} \min(e_i, e_j) r_i r_j = n. \qquad (4)$$

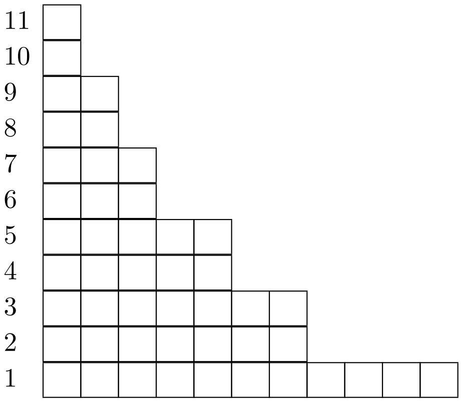
We denote by $\underline{e} \in \mathcal{P}_G$ the partition that is formed by the e_i (counted with multiplicities r_i).
Now we compute $\underline{\tilde{\lambda}} := \iota(\underline{e}) \in \mathcal{P}_{base}$ from $\underline{e}$. (See 6.1 for the exact mapping). Let $\underline{\tilde{\lambda}} = (\tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3, \ldots, \tilde{\lambda}_{2k+1})$. One checks that

$$\sum_{i,j} \min(e_i, e_j) r_i r_j = \sum_{i=1}^{2k+1} \tilde{\lambda}_i.$$

Thus equation (4) looks:

$$\sum_{i,s} s b_{i,s} + \sum_{i=1}^{2k+1} \tilde{\lambda}_i = n. \qquad (5)$$

The introduction of $\underline{\tilde{\lambda}}$ and the preceding formula, though easy to verify, seem rather poorly motivated. If the reader returns to Example 4.5, the “remainder” $\underline{n}_7$ is a partition in $\mathcal{P}_{base}$, namely $\underline{n}_7 = \underline{\tilde{\lambda}}$ (cf. diagram below). Since $\underline{n}$ consists of these boxes and of the boxes that were removed (counted by the a_i), the connection to the term $\sum_{i=1}^{2k+1} \tilde{\lambda}_i$ in equation (5) becomes obvious.



On the other hand, if we start with some partition of n, the algorithm yields a sequence $\lambda_k \leq \lambda_{k-1} \leq \ldots \leq \lambda_1$. Furthermore, we get (a_i), $1 \leq i \leq k$ (cf. Remark 4.4). It is easy to see that if $\lambda_i = \lambda_{i+1}$, then $a_i \geq a_{i+1}$. Hence, if we have a sequence $\lambda_1 = \lambda_2 = \ldots = \lambda_{r_1}$ of r_1 equal terms, we also get a monotone sequence $a_1 \geq a_2 \geq \ldots \geq a_{r_1}$. By defining $b_{1,s} := a_s - a_{s-1}$ $(a_0 := 0)$, we get numbers which satisfy

$$\sum_{s=1}^{r_1} s b_{1,s} = \sum_{i=1}^{r_1} a_i.$$

In the same way, we can define $b_{i,s}$ for the other i.

Now we define $\underline{\tilde{\lambda}} = (\tilde{\lambda_1}, \ldots, \tilde{\lambda_{2k+1}})$ as the image $\iota(\underline{\lambda})$ of $\underline{\lambda}$ in $\mathcal{P}_{base}$. Then it is immediate to check that

$$\sum_{i=1}^{k} \lambda_i (2i-1) = \sum_{i=1}^{2k+1} \tilde{\lambda_i}.$$

We recall that

$$\begin{aligned} n &= \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} \lambda_i (2i-1) \\ &= \sum_{i,s} s b_{i,s} + \sum_{i=1}^{2k+1} \tilde{\lambda_i}, \end{aligned}$$

which is exactly equation (5).

So we have seen that each partition $\underline{n}$ of n with $\Lambda(\underline{n}) = \underline{e} \in \mathcal{P}_G$ corresponds to a solution $(b_{i,s})_{i,s}$ of equation (4). On the other hand, given such a solution $(b_{i,s})_{i,s}$, we can compute the data λ_i and a_i. But given these data, we can reverse every single step of the algorithm, so we can recover the partition $\underline{n}$.

Altogether, the terms in (3) contributing to q^n are in bijection with the partitions $\underline{n}$ of n with $\Lambda(\underline{n}) = \underline{e}$, which proves the claim. □

7 Some consequences

Theorem (3.1) enables us to compute the probability of a group to have a certain exponent. To simplify notation, I use the p-logarithmic exponent, i.e., *if a p-group has exponent e, I mean that it is annihilated by p^e.*

7.1 Theorem. *Let $e \geq 0$ be fixed. Then we have*

$$\sum_{\substack{G \text{ is a } p\text{-group} \\ \text{of exponent } \leq e}} w(G) = \prod_{\substack{j \not\equiv 0, \pm(e+1) \\ \bmod 2e+3}} (1-q^j)^{-1}.$$

(Note that j runs through all positive integers, not only through all residue classes $\bmod 2e+3$.)

Proof. Recall that, by the main theorem,

$$w(G) = \sum_{n \geq 0} a_G(n) q^n,$$

where

$$a_G(n) = \left| \Lambda^{-1}(G) \cap \{\underline{n} \in \mathcal{P} | \ \underline{n} \text{ is a partition of } n \in \mathbb{N}\} \right|.$$

Hence,

$$\sum_{\substack{G \text{ is a } p\text{-group} \\ \text{of exponent } \leq e}} w(G) = \sum_{n \geq 0} \left| \left\{ \underline{n} \in \mathcal{P} | \ \begin{array}{c} \underline{n} \text{ is a partition of } n \text{ and} \\ \Lambda(\underline{n}) \text{ has exponent } \leq e \end{array} \right\} \right| q^n.$$

But if G is interpreted as a partition in $\mathcal{P}_G$, then the exponent is simply the largest part. Given a partition $\underline{n} = (n_1, \ldots, n_m) \in \mathcal{P}$, the largest part of $\Lambda(\underline{n})$ will be λ_1, since the λ_i are sorted. On the other hand, it is easy to see that $\lambda_1 = \max_i (n_{i+2} - n_i)$. So we know that

$$\sum_{\substack{G \text{ is a } p\text{-group} \\ \text{of exponent } \leq e}} w(G) = \sum_{n \geq 0} \left| \left\{ \underline{n} = (n_1, \ldots, n_m) \in \mathcal{P} | \ \begin{array}{c} \underline{n} \text{ is a partition of n and} \\ n_{i+2} - n_i \leq e \text{ for all } i \end{array} \right\} \right| q^n,$$

where again we put $n_0 = n_{-1} = 0$. But the right hand side is a well-known generating function, and its value is

$$\prod_{\substack{j \not\equiv 0, \pm(e+1) \\ \bmod 2e+3}} (1-q^j)^{-1}$$

(cf. [1], Thm 7.5, $k := i := e+1$), which proves the theorem. □

7.2 Corollary. *The probability (in the Cohen-Lenstra heuristic) that a p-group has exponent $\leq e$ is*

$$\prod_{\substack{j \equiv 0, \pm(e+1) \\ \bmod 2e+3}} (1-p^{-j}).$$

Proof. The heuristic tells us that the volume of the one-element set $\{G\}$ is $\frac{w(G)}{\eta_\infty(p)}$ (here $w(G)$ is interpreted as an evaluated, not a formal series), so the probability of a p-group having exponent $\leq e$ is

$$\begin{aligned}\frac{1}{\eta_\infty(p)}\left(\sum_{\substack{G \text{ is a } p\text{-group} \\ \text{of exponent } \leq e}} w(G)\right) &= \left(\prod_{j\geq 1}(1-p^{-j})\right)\left(\prod_{\substack{j\not\equiv 0,\pm(e+1) \\ \bmod 2e+3}}(1-p^{-j})^{-1}\right) \\ &= \prod_{\substack{j\equiv 0,\pm(e+1) \\ \bmod 2e+3}}(1-p^{-j}).\end{aligned}$$

□

To give a feeling for those probabilities, here is a table that lists the probability for a finite abelian p-group to have p-exponent e.

	$e=0$	$e=1$	$e=2$	$e=3$	$e>4$
$p=2$	28.879%	33.965%	18.521%	9.361%	9.374%
$p=3$	56.013%	29.178%	9.871%	3.292%	1.646%
$p=5$	76.033%	19.167%	3.840%	0.768%	0.192%
$p=7$	83.680%	13.988%	1.999%	0.286%	0.048%
$p=11$	90.083%	9.015%	0.820%	0.075%	0.007%

7.3 Remark. This corollary is a generalisation of [2, Example 5.3], where the case $e=1$ is treated. Also, similar formulas for the rank of a p-group are known ([2, Thm. 6.1]). However, rank and exponent behave rather antipodal: It is pretty straightforward to derive results about the rank from the original Cohen-Lenstra approach, but the exponent gives very tough problems (except for $e=1$).

On the other hand, with the given partition-theoretic interpretation (Theorem 3.1), the exponent formula above is an almost trivial consequence, whereas it is not clear at all what it means for a partition to be mapped under Λ to a group of some given rank.

References

[1] G.E. Andrews, The Theory of Partitions, Encyclopedia of Mathematics and its Applications, Vol. **2**, Addison-Wesley Publishing Company, Reading, Massachusets, 1976

[2] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields, Number Theory Noordwijkerhout (H. Jager, ed.), Lecture Notes in Math. vol. **1068**, Springer-Verlag, Berlin and New York, 1984, pp. 33-62.

[3] E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over finite fields, Theorie des Nombres,

Proc. Int. Number Theory Conf. Laval, 1987. Walter de Gruyter, Berlin and New York (1989) pp. 227-239.