Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 176

A formula for the probability of the exponents of finite p-groups

Johannes Lengler

Saarbrücken 2006

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 176
submitted: June 27, 2006

A formula for the probability of the exponents of finite p-groups

Johannes Lengler

Saarland University
Department of Mathematics
P.O. Box 15 11 50
66041 Saarbrücken
Germany
johnny@math.uni-sb.de

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

Abstract

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

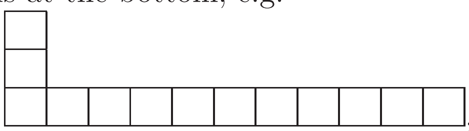
Contents

1 Preliminaries and Motivation

I assume that the reader is familiar with (or accepts) the following facts:

- 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 $(1, 1, 11)$. The total number of boxes corresponds to the number that is partitioned, in the example $13 = 1 + 1 + 11$.

- 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 $\eta_\infty(p)\frac{1}{|\mathrm{Aut}(G)|}$ (cf. [CL], [FW]).
  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
$$|\mathrm{Aut}(G)| = \left(\prod_{i=1}^{k}\left(\prod_{j=1}^{r_i}(1-p^{-j})\right)\right)\left(\prod_{1\le i,j\le k} p^{\min(e_i,e_j)r_ir_j}\right).$$

If we put $X := p^{-1}$, the *weight of* G is the formal power series
$$w(G) := \left(\prod_{i=1}^{k}\left(\prod_{j=1}^{r_i}(1-X^{j})^{-1}\right)\right)\left(\prod_{1\le i,j\le k} X^{\min(e_i,e_j)r_ir_j}\right).$$

This agrees with the notation in the Cohen-Lenstra paper [CL], except that here I work with formal power series whereas Cohen and Lenstra work with evaluated series. However, it is always possible to replace X by p^{-1}, so (hopefully) no confusion will arise.

Note that
$$\sum_G w(G) \ = \ \prod_{i=1}^{\infty}(1-X^i)^{-1} = \sum_{n\in\mathbb{N}} p(n)X^n = \sum_{n\in\mathbb{N}} \sum_{\substack{\underline{n} \text{ is a par-}\\ \text{tition of } n}} X^n,$$
where $p(n)$ is the number of partitions of n. (As usual, $p(0) = 1$.)
We see that, quite naturally, partitions come into play. We see further that both sides of the equation are sums, one taken over all (p-)groups G, the other one taken over all partitions. On the left hand side, each term is a formal power series in X, whereas on the right hand side, each term is just a monomial X^n.
So it is not farfetched to suspect 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 decompostion 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) map π 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.

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 $\mathcal{P}$. A partition in $\mathcal{P}_G$ will be identified with its corresponding group.
  If I use placeholders for partitions, I will usually flag them with an underscore, e.g. $\underline{n} = (1, 1, 11)$.

2 The statement

The article is devoted to defining a map $\pi : \mathcal{P} \to \mathcal{P}_G$ with the following property:

2.1 Theorem. *For a finite p-group G, the mapping π defined in sections 3 and 4 can be used to compute $w(G)$ via:*

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

where

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

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

Hence, π has the properties announced in the introduction.

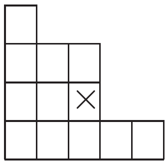
A proof of the theorem will follow in section 6.
Beforehand of course, I have to define the mapping π. This will be done in two ways: via Young tableaux and numerically. The next two chapters are devoted to this purpose.

3 Definition of π (via Young tableaux)

So let us turn to the definition of the mapping π.
First I introduce a new (non-standard) notation:

3.1 Notation.

- In the Young Tableau, we denote by $(i, j) \in \mathbb{N} \times \mathbb{N}$ 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 π can be defined by the following algorithm:

3.2 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 $\pi(\underline{n}) := (\lambda_k, \lambda_{k-1}, \ldots, \lambda_1) \in \mathcal{P}_G$.

3.3 Remark.

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

- The λ_i are sorted: $\lambda_1 \geq \ldots \geq \lambda_k$.

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.

3.4 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 $n = \left(\sum_{i=1}^{k} \lambda_i(2i-1)\right) + \sum_{i=1}^{k} a_i$.

3.5 Remark. This version of the algorithm is harder to understand than the numerical version in the next section. However, the following example not only shows how the algorithm works. It also indicates why such mysterious objects as the a_i or $\mathcal{P}_{base}$ (see section 6) appear in the proof of Theorem 2.1.

3.6 Example. Space limitations don't allow to illustrate the algorithm graphically. So I will just give the main variables and leave it to the reader to draw the diagrams. 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. Let us consider the partition $\underline{n} = (1,1,2,3,4,4,4,6,8,8,9,9,9,11,11)$.
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 $(9,5) \notin M_1$.

By computing step 4 of the algorithm we get the partition

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

Note that the algorithm does not tell us what the last two terms of $\underline{\text{n}}$ are. This is okay because it will not have any influence on the further steps of the algorithm. Manipulating the process like this will make the proof in section 6 a bit clearer : In this way, the remaining partition $\underline{n}_7$ will be an element of $\mathcal{P}_{base}$ (see definition in section 6) and the number of removed boxes $n_i - n_{i+1}$ will equal a_i. (n_i denotes the number that is partitioned by $\underline{n}_i$.)

If the reader is not interested in the proof, he/she may ignore these data.

Now we find that $\lambda_2 = 2$ and $i_2 = 3$ and obtain

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

Again, the reader who is not interested in the proof may ignore the last four entries. 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 $\lambda_4 = 1$, $i_4 = 15$:

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

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

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

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:

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

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

4 Definition of π (numerical)

4.1 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 $\overline{n} = (\overline{n}_1, \overline{n}_2, \ldots \overline{n}_m)$, 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 $\lambda_k := \max_l \{\overline{n}^k_l\}$, and let $i_k := \min\{l | \ \overline{n}^k_l = \lambda_k\}$.*

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 $\overline{n}^k_{i_k-1}+\overline{n}^k_{i_k+1}-\overline{n}^k_{i_k}$, thereby getting $\overline{n}^{k+1}$. Increase k by 1.*
   (We might need to use some $\overline{n}^k_l$ 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 $(\lambda_k, \lambda_{k-1}, \lambda_{k-2}, \ldots, \lambda_1) \in \mathcal{P}_G$.

4.2 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 $\overline{n}^k_{i-1}+\overline{n}^k_{i+1} \geq \overline{n}^k_i$ 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. However, I decided to include both variants because in this version it would be harder to see the relationship (Thm. 2.1) between the Cohen-Lenstra probability measure for p-groups and the mapping π.

4.3 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 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$.

5 Some consequences

Now we are able 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.*

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

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

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

Proof. Recall that, by the main theorem,

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

where

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

Hence,

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

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

$\pi(\underline{n})$ 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

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

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

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

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

5.2 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

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

$\square$

5.3 Remark. This corollary is a generalisation of [CL, Example 5.3], where the case $e = 1$ is treated. Also, similar formulas for the rank of a p-group are known ([CL, 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 $e = 1$).
Vice versa, with the given partition-theoretic interpretation (Theorem 2.1), 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 π to a group of some given rank.

6 Proof of Theorem 2.1

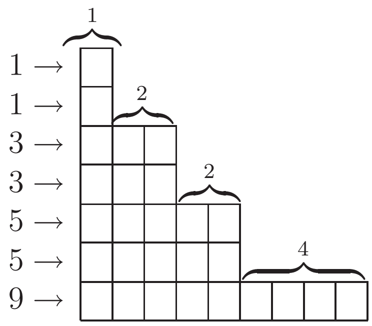
The set $\mathcal{P}_{base} \subset \mathcal{P}$ will under π correspond one-to-one with the set $\mathcal{P}_G$ of all partitions. I will define it by constructing an (injective) section $\iota : \mathcal{P}_G \to \mathcal{P}$, i.e., $\pi \circ \iota = id_{\mathcal{P}_G}$. Then, $\mathcal{P}_{base}$ 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 $\underline{n} = (n_1, n_2, \ldots, n_k) \in \mathcal{P}_G$, $0 < n_1 \le n_2 \le \ldots \le n_k$. Then its corresponding element $\iota(\underline{n}) \in \mathcal{P}_{base}$ is defined as the partition

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

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

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 (2.1).
In Remark 3.4, I introduced numbers a_i, which were illustrated in the succeeding example. Recall that 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

$$w(G) = \left(\prod_{i=1}^{k} \left(\prod_{j=1}^{r_i} (1 - X^j)^{-1}\right)\right) \left(\prod_{1 \le i,j \le k} X^{\min(e_i,e_j) r_i r_j}\right). \tag{2}$$

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

$$\sum_{i,j} j b_{i,j} + \sum_{i,j} \min(e_i, e_j) r_i r_j = n. \tag{3}$$

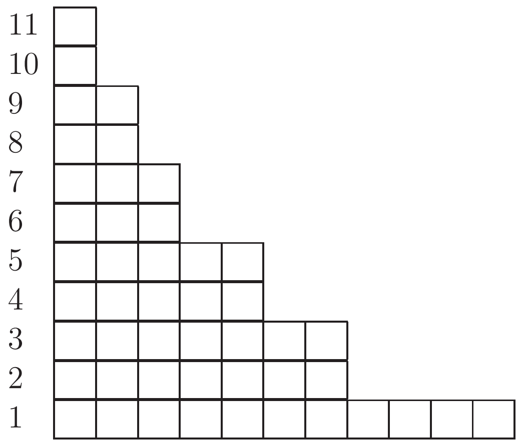
We denote by $\underline{e} \in \mathcal{P}_G$ the partition that is formed by the e_i (counted with multiplicities r_i).
Now we compute $\underline{\tilde{\lambda}} := \iota(\underline{e}) \in \mathcal{P}_{base}$ from $\underline{e}$. (See 6.1 for the exact mapping). Let $\underline{\tilde{\lambda}}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

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

Thus equation (3) looks:

$$\sum_{i,j} j b_{i,j} + \sum_{j=1}^{k} \tilde{\lambda}_i = n. \tag{4}$$

The introduction of $\underline{\tilde{\lambda}}$ and the preceding formula, though easy to verify, seem rather poorly motivated. If the reader returns to Example 3.6, 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 $\sum_{i=1}^{k} \tilde{\lambda}_i$ in equation (4) 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 3.4). 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 $b_{1,j} := a_j - a_{j-1}$ ($a_0 := 0$), we get numbers which satisfy

$$\sum_{j=1}^{r_1} j b_{1,j} = \sum_{j=1}^{r_1} a_j.$$

In the same way, we can define $b_{i,j}$ for the other i.
Now, we define $\underline{\tilde{\lambda}} = (\tilde{\lambda_1}, \ldots, \tilde{\lambda_k})$ as the image $\iota(\underline{\lambda})$ of $\underline{\lambda}$ in $\mathcal{P}_{base}$. Then it is immediate to check that

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

We recall that

$$\begin{aligned} n &= \sum_{j=1}^{r_1} a_j + \sum_{j=1}^{k} \lambda_i(2i-1) \\ &= \sum_{j=1}^{r_1} j b_{1,j} + \sum_{j=1}^{k} \tilde{\lambda_i}, \end{aligned}$$

which is exactly equation (4).
So we have seen that each partition $\underline{n}$ of n with $\pi(\underline{n}) = \underline{e} \in \mathcal{P}_G$ corresponds to a solution $(b_{i,j})_{i,j}$ of equation (3). On the other hand, given such a solution $(b_{i,j})_{i,j}$, 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 (2) contributing to X^n are in bijection with the partitions $\underline{n}$ of n with $\pi(\underline{n}) = \underline{e}$, which proves the claim. $\square$

References

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

[CL] *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.*

[FW] *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.*