Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Permuting the partitions of a prime

par Stéphane VINATIER

Résumé. Étant donné un nombre premier p impair, on caractérise les partitions $\underline{\ell}$ de p à p parts *positives ou nulles* $\ell_0 \geq \ell_1 \geq \ldots \geq \ell_{p-1} \geq 0$ pour lesquelles il existe des permutations σ, τ de l'ensemble $\{0, \ldots, p-1\}$ telles que p divise $\sum_{i=0}^{p-1} i\ell_{\sigma(i)}$ mais ne divise pas $\sum_{i=0}^{p-1} i\ell_{\tau(i)}$. Cela se produit si et seulement si le nombre maximal de parts égales de $\underline{\ell}$ est strictement inférieur à $p-2$. Cette question est apparue en manipulant des sommes de puissances p-ièmes de résolvantes, en lien avec un problème de structure galoisienne.

Abstract. Given an odd prime number p, we characterize the partitions $\underline{\ell}$ of p with p *non negative* parts $\ell_0 \geq \ell_1 \geq \ldots \geq \ell_{p-1} \geq 0$ for which there exist permutations σ, τ of the set $\{0, \ldots, p-1\}$ such that p divides $\sum_{i=0}^{p-1} i\ell_{\sigma(i)}$ but does not divide $\sum_{i=0}^{p-1} i\ell_{\tau(i)}$. This happens if and only if the maximal number of equal parts of $\underline{\ell}$ is less than $p-2$. The question appeared when dealing with sums of p-th powers of resolvents, in order to solve a Galois module structure problem.

1. Formulation of the main result

Let p denote an odd prime number and consider the set $\mathcal{C}$ of all p-uples $\underline{\ell} = (\ell_0, \ell_1, \ldots, \ell_{p-1})$ of non negative integers such that

$$\ell_0 + \ell_1 + \cdots + \ell_{p-1} = p \ .$$

We call the elements of the set $\mathcal{C}$ the *compositions* of p and the integers ℓ_i appearing in the composition $\underline{\ell}$ its *parts*, even for the zero ones. The *length* of the composition $\underline{\ell}$ is the number of its non zero parts.

Let $\mathfrak{S}$ denote the permutation group of $\{0, 1, \ldots, p-1\}$. We let $\mathfrak{S}$ act on $\mathcal{C}$ through its action on the indices of the compositions:

$$\sigma(\underline{\ell}) = (\ell_{\sigma(0)}, \ell_{\sigma(1)}, \ldots, \ell_{\sigma(p-1)})$$

for all $\sigma \in \mathfrak{S}$, $\underline{\ell} \in \mathcal{C}$. Each coset of $\mathcal{C}$ for this action has a unique representative with non increasing parts:

$$\ell_0 \geq \ell_1 \geq \cdots \geq \ell_{p-1} \ ;$$

such a composition is called a *partition* of p. We shall also call *partition* its coset and we let $\mathcal{P}$ denote the set of all partitions of p.

Given a composition $\underline{\ell}$, we are interested in the divisibility by p of the sum $S(\underline{\ell})$ of its parts multiplied by their index:

$$S(\underline{\ell}) = \sum_{i=0}^{p-1} i\ell_i \ .$$

(0) *AMS Mathematical Subject Classification 2000: 05A17; 05A10; 11P83. Keywords: partitions of a prime; sums of resolvents; multinomials.*

The main result of this paper is a characterization of the cosets that contain compositions $\underline{\ell}$ for which $S(\underline{\ell})$ is divisible by p and compositions for which it is not. In other words, we are interested in determining those partitions $\underline{\ell} \in \mathcal{P}$ such that:

$$\exists\ \sigma, \tau \in \mathfrak{S}, \quad p \mid S(\sigma(\underline{\ell})) \quad \text{and} \quad p \nmid S(\tau(\underline{\ell}))\ . \tag{1}$$

Considering the most basic partitions of p, $(p, 0, \dots, 0)$ and $(1, \dots, 1)$, one sees at once that p divides $S(\sigma(\underline{\ell}))$ for all $\sigma \in \mathfrak{S}$ in both cases. At the contrary, using the fact that p is prime, one checks that p never divides $S(\sigma(\underline{\ell}))$ when $\underline{\ell}$ is chosen among the partitions of the kind $(p-k, k, 0, \dots, 0)$, $1 \leq k \leq \frac{p-1}{2}$ or $\underline{\ell} = (2, 1, \dots, 1, 0)$. All these "basic" partitions are clearly characterized by the fact that their *maximal number of equal parts*, denoted $m(\underline{\ell})$, is at least $p-2$. Indeed the main result states that they are the only ones that do not satisfy condition (1).

In order to get one further characterization, let $e_k(\underline{\ell})$ denote, for $0 \leq k \leq p$, the number of parts of $\underline{\ell}$ equal to k:

$$e_k(\underline{\ell}) = \#\{0 \leq i \leq p-1 \mid \ell_i = k\}\ .$$

Obviously, $m(\underline{\ell}) = \max\{e_k(\underline{\ell}),\ 0 \leq k \leq p-1\}$. Consider the p-uple:

$$\underline{e}(\underline{\ell}) = \big(e_0(\underline{\ell}), \dots, e_{p-1}(\underline{\ell})\big)\ .$$

If $\underline{\ell}$ is distinct from $(p, 0, \dots, 0)$, all its parts are less than p; their total number is always p in our setting, therefore $\underline{e}(\underline{\ell})$ is a composition of p, namely

$$\sum_{k=0}^{p-1} e_k(\underline{\ell}) = p\ .$$

Further we note $\underline{e}(\underline{\ell})! = e_0(\underline{\ell})! \cdot e_1(\underline{\ell})! \cdots e_{p-1}(\underline{\ell})!$; this expression equals the cardinal of the stabilizer of $\underline{\ell}$ under the action of $\mathfrak{S}$. The main result is as follows.

Theorem. *Let $\underline{\ell}$ be a partition of p. The following assertions are equivalent:*

(i) $\exists\ \sigma, \tau \in \mathfrak{S}$ *such that* $p \mid S(\sigma(\underline{\ell}))$ *and* $p \nmid S(\tau(\underline{\ell}))$;
(ii) $m(\underline{\ell}) < p-2$;
(iii) $\underline{e}(\underline{\ell})! < (p-2)!$.

We prove the Theorem in section 3. The heart of the proof is Lemma 3.2, which is proven in two parts, depending on the length of $\underline{\ell}$, both elementary. One more characterization, involving a larger family of partitions, will be given in section 4.

Such problems about "permuted partitions" do not seem to have appeared in combinatorics or in number theory so far; in particular, the very rich account on the theory of partitions by Andrews [A] does not mention such questions. In section 2, we explain how this problem came up while trying to compute sums of p-th powers of resolvents (in order to solve a Galois module structure question), starting from case $p = 3$ where the computation is a part of Lagrange's resolvent method to solve the general cubic equation.

Applications of this result will be given in a forthcoming paper, in terms of arrangements of hyperplanes over the finite field with p elements $\mathbb{F}_p$.

2. A motivation for the main result

Lagrange's resolvent method for the cubic equation has the following pattern. Let t_0, t_1, t_2 denote the roots of a given monic cubic polynomial P in some fixed algebraic closure of the base field, let ζ denote a primitive cubic root of unity and define

$$y = t_0 + \zeta t_1 + \zeta^2 t_2 \ , \ z = t_0 + \zeta^2 t_1 + \zeta t_2 \ .$$

Then y^3 and z^3, the *Lagrange resolvents*, are the roots of a polynomial of degree 2 which coefficients are invariant under the permutation group of $\{t_0, t_1, t_2\}$, hence can be expressed in terms of the coefficients of P. Therefore y^3 and z^3 have an expression in terms of these coefficients, from which one easily deduces one for t_0, t_1, t_2 (see [DM] for technical and historical details). The coefficients of the degree 2 polynomial are y^3+z^3 and y^3z^3 and are both easy to compute. In particular,

$$y^3 + z^3 = 2\sigma_1^3 - 9\sigma_1\sigma_2 + 27\sigma_3 \ ,$$

where $\sigma_1, \sigma_2, \sigma_3$ denote the elementary symmetric functions of the roots and equal the coefficients of P modulo a sign.

Considering the analogous computation when 3 is replaced by any odd prime p may be of some interest. Given p algebraic numbers[(1)] $t_0, t_1, \ldots, t_{p-1}$ and a primitive p-th root of unity ζ, one may define *generalized resolvents*

$$y_k = \sum_{i=0}^{p-1} \zeta^{ik} t_i \ , \quad 1 \leq k \leq p-1 \ ,$$

and may be willing to compute the sum of their p-th powers

$$y_1^p + y_2^p + \cdots + y_{p-1}^p = \sum_{k=1}^{p-1} \Big(\sum_{i=0}^{p-1} \zeta^{ik} t_i \Big)^p \ .$$

Of course for p greater than 3, this expression is no longer symmetric under the permutation group of $\{t_0, \ldots, t_{p-1}\}$, hence not expressible in terms of the elementary symmetric functions. Yet a sum of such expressions appears in [V], and it is shown that its valuation at p bears information about the Galois module structure of the "square root of the inverse different" ideal of a weakly ramified p-extension of the rationals. In that paper, the author was able to achieve the computation only in the case $p = 3$, using the above calculation.

Developping the p-th power with the help of Newton's multinomial formula yields

$$y_1^p + \cdots + y_{p-1}^p = \sum_{k=1}^{p-1} \sum_{\underline{\ell} \in \mathcal{C}} \frac{p!}{\underline{\ell}!} \prod_{i=0}^{p-1} \left(\zeta^{ik} t_i \right)^{\ell_i},$$

where we let $\underline{\ell}!$ denote the product of the factorials of the parts of $\underline{\ell}$:

$$\underline{\ell}! = \ell_0! \cdot \ell_1! \cdots \ell_{p-1}! \ ,$$

so $p!/\underline{\ell}!$ equals the multinomial coefficient $\binom{p}{\ell_0, \ldots, \ell_{p-1}}$. Since this coefficient only depends on the partition containing $\underline{\ell}$, we index the second sum by partitions instead of compositions and use the action of $\mathfrak{S}$ on partitions to recover all the compositions. Taking into account the fact that a composition

(1) $t_0, t_1, \ldots, t_{p-1}$ may equally be considered as indeterminates in fact.

$\underline{\ell}$ is fixed by exactly $\underline{e}(\underline{\ell})!$ permutations (this number also only depends on the partition containing $\underline{\ell}$), we get

$$y_1^p + \cdots + y_{p-1}^p = \sum_{k=1}^{p-1} \sum_{\mathcal{P}\times\mathfrak{S}} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!} \Big(\prod_{i=0}^{p-1} \big(\zeta^{ik} t_i\big)^{\ell_{\sigma(i)}} \Big) \ ,$$

where the second sum is on couples $(\underline{\ell}, \sigma) \in \mathcal{P} \times \mathfrak{S}$. Further

$$\prod_{i=0}^{p-1} \big(\zeta^{ik} t_i\big)^{\ell_{\sigma(i)}} = \zeta^{k\sum_{i=0}^{p-1} i\ell_{\sigma(i)}} \cdot \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \ \text{ and } \ \sum_{k=1}^{p-1} \zeta^{k\sum_{i=0}^{p-1} i\ell_{\sigma(i)}} = p-1 \text{ or } -1 \ ,$$

depending on whether p divides $S(\sigma(\underline{\ell})) = \sum_{i=0}^{p-1} i\ell_{\sigma(i)}$ or not, hence

$$\begin{aligned} y_1^p + \cdots + y_{p-1}^p &= \sum_{\mathcal{P}\times\mathfrak{S}} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!} \Big(\prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \Big) \Big(\sum_{k=1}^{p-1} \zeta^{k\sum_{i=0}^{p-1} i\ell_{\sigma(i)}} \Big) \\ &= (p-1) \sum_{\mathcal{P}\times\mathfrak{S}} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!} \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \ - \ p \sum_{(\mathcal{P}\times\mathfrak{S})^*} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!} \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \\ &= (p-1)(t_0 + \cdots + t_{p-1})^p \ - \ p \sum_{(\mathcal{P}\times\mathfrak{S})^*} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!} \prod_{i=0}^{p-1} t_{\sigma^{-1}(i)}^{\ell_i} \ , \end{aligned}$$

where in each second sum, $(\underline{\ell}, \sigma)$ runs among the couples in $\mathcal{P} \times \mathfrak{S}$ such that p does not divide $S(\sigma(\underline{\ell}))$.

It now clearly appears that the non-symmetric aspect of the expression $y_1^p + \cdots + y_{p-1}^p$ is linked to the existence of partitions of p satisfying condition (1). This happens as soon as p is greater than 3, as is easily deduced from the Theorem, for which we shall now give a proof.

3. The proof of the main result

Let $\underline{\ell}$ denote a partition of p. Recall that the Theorem states the equivalence of the following assertions:

(i) $\exists\ \sigma, \tau \in \mathfrak{S}$ *such that* $p \mid S(\sigma(\underline{\ell}))$ *and* $p \nmid S(\tau(\underline{\ell}))$;
(ii) *the maximal number of equal parts of* $\underline{\ell}$ *satisfies:* $m(\underline{\ell}) < p-2$;
(iii) *the cardinal of the stabilizer of* $\underline{\ell}$ *under* $\mathfrak{S}$ *satisfies:* $\underline{e}(\underline{\ell})! < (p-2)!$.

Proof. First assume assertion (ii) is not satisfied, namely $m(\underline{\ell}) \geq p-2$, then $m(\underline{\ell}) = e_0(\underline{\ell})$ or $e_1(\underline{\ell})$, and $\underline{\ell}$ is one of the "basic partitions" listed above the Theorem in section 1, hence does not satisfy assertion (i). Further $m(\underline{\ell})! \mid \underline{e}(\underline{\ell})!$, hence (iii) is not satisfied either.

Let us show now that (ii) $\Rightarrow$ (iii). First notice that (ii) never occurs when $p = 3$. If $p \in \{5, 7\}$, the implication is easily verified by considering each partition of p separately. For the general case we use the following result.

Lemma 3.1. *Assume* $p \geq 11$. *Let* $\underline{d} = (d_0, \ldots, d_{p-1})$ *be a partition of* p *of length* s, *such that* $d_i \leq p-3$ *for all* i, *then*

$$\frac{p!}{\underline{d}!} > 2^{s-2} p(p-1) \ .$$

Proof. We shall prove the lemma by induction on s. The case $s = 1$ is irrelevant here. If $s = 2$, $\frac{p!}{\underline{d}!}$ equals the binomial coefficient $\binom{p}{d_0}$. Since

$3 \leq d_0 \leq p-3$,

$$\binom{p}{d_0} \geq \binom{p}{3} = p(p-1)\frac{p-2}{6} \ .$$

Further $\frac{p-2}{6} > 1$ when $p > 8$, hence the result.

Assume the result is true for some $s \geq 2$ and let $\underline{d} = (d_0, \ldots, d_s, 0, \ldots, 0)$ denote a partition of p with $s+1$ non zero parts, all at most $p-3$. Then we claim that $d_{s-1} + d_s \leq p-3$. Otherwise, one would have $d_i \geq \frac{d_{s-1}+d_s}{2} > \frac{p-3}{2}$ for all $0 \leq i \leq s-1$, and

$$p = (d_0 + \cdots + d_{s-2}) + (d_{s-1} + d_s) > (s-1)\frac{p-3}{2} + (p-3) \ ,$$

which implies $p < 3 + \frac{6}{s-1} \leq 9$ and contradicts our hypothesis about p. We apply the induction hypothesis to the partition in the coset of $(d_0, \ldots, d_{s-2}, d_{s-1} + d_s, 0, \ldots, 0)$, it yields

$$\frac{p!}{\underline{d}!} = \frac{p!}{d_0! \ldots d_{s-2}!(d_{s-1}+d_s)!}\frac{(d_{s-1}+d_s)!}{d_{s-1}!d_s!} > 2^{s-2}p(p-1)\frac{(d_{s-1}+d_s)!}{d_{s-1}!d_s!} \ .$$

Notice that $\frac{(d_{s-1}+d_s)!}{d_{s-1}!d_s!} \geq d_{s-1} + d_s \geq 2$ to end the proof of the lemma. □

Under assertion (ii), $\underline{\ell}$ is distinct from $(p, 0 \ldots, 0)$, hence we may consider the partition $\underline{d}$ of p in the coset of $\underline{e}(\underline{\ell})$; since $m(\underline{\ell}) = \max\{e_k(\ell), 0 \leq k \leq p-1\}$, all the parts of $\underline{d}$ are less than $p-2$ (and s is at least 2). The lemma yields:

$$\underline{e}(\underline{\ell})! = \underline{d}! < \frac{(p-2)!}{2^{s-2}} \ ,$$

hence assertion (iii) is verified.

We now have to prove (ii) ⇒ (i). We assume again $p \neq 3$ and we denote by s the length of $\underline{\ell}$; then $s = p - e_0(\underline{\ell})$ and one easily checks that, under condition (ii), $3 \leq s \leq p-2$.

Lemma 3.2. *Let $\underline{\ell}$ be a partition of p with length s satisfying $3 \leq s \leq p-2$. Then there exist s distinct numbers $a_0, \ldots, a_{s-1} \in \{0, \ldots, p-1\}$ such that*

$$a_0\ell_0 + \cdots + a_{s-1}\ell_{s-1} \equiv 0 \mod p \ .$$

Proof. We first prove the assertion for $3 \leq s \leq \frac{p+1}{2}$ by induction on s. If $s = 3$, take any $a_0 \in \{0, \ldots, p-1\}$, then let $a_1, a_2 \in \{0, \ldots, p-1\}$ be such that $a_1 \equiv \ell_2 + a_0 \mod p$ and $a_2 \equiv -\ell_1 + a_0 \mod p$ to get the result.

Assume the assertion is true for the partitions of p of length $s-1$ ($s \geq 4$). Then there exist $s-1$ distinct numbers $a_0, \ldots, a_{s-2}$ in $\{0, \ldots, p-1\}$ such that

$$a_0\ell_0 + \cdots + a_{s-2}(\ell_{s-2} + \ell_{s-1}) \equiv 0 \mod p \ .$$

Further we may assume $a_{s-2} \neq 0$, since the same relation is satisfied by the numbers $a_0 + 1, \ldots, a_{s-2} + 1$. Let d denote the greatest common divisor of ℓ_{s-2} and ℓ_{s-1}, and let $a, b \in \mathbb{Z}$ be such that $a\ell_{s-2} + b\ell_{s-1} = d$ (Bézout relationship); further let $\alpha = \frac{\ell_{s-2}}{d}$, $\beta = \frac{\ell_{s-1}}{d}$ and $\gamma = \alpha + \beta$. Then the couples $(x, y) \in \mathbb{Z}^2$ satisfying $x\ell_{s-2} + y\ell_{s-1} = d$ are exactly those for which there exists $n \in \mathbb{Z}$ such that $x = a - n\beta$ and $y = b + n\alpha$. Since α and β are invertible modulo p, x and y may take any value modulo p. Further

$$x \equiv y \mod p \Leftrightarrow \gamma n \equiv a - b \mod p \ ,$$

hence $x \not\equiv y \mod p$ occurs for $p-1$ values of the residue of n modulo p. Eventually, $a_{s-2}(\ell_{s-2}+\ell_{s-1}) = a_{s-2}\gamma d = a_{s-2}\gamma x\ell_{s-2} + a_{s-2}\gamma y\ell_{s-1}$ and $a_{s-2}\gamma x \not\equiv a_{s-2}\gamma y \mod p$ simultaneously occur for $p-1$ couples $(x,y) \in \{0,\dots,p-1\}^2$. There remain $p-1-(s-2)$ such couples if one requires further that $a_{s-2}\gamma x \not\equiv a_0,\dots,a_{s-3} \mod p$. Since $s \leq \frac{p+1}{2}$ implies $p-1-(s-2) > s-2$, at least one of the values of y is such that $a_{s-2}\gamma y$ is also distinct from the $a_i \mod p$ for $0 \leq i \leq s-3$, hence the result when $s \leq \frac{p+1}{2}$.

We now consider the case $\frac{p+3}{2} \leq s \leq p-2$. This assumption is equivalent to

$$2 \leq e_0(\underline{\ell}) = p - s \leq \frac{p-3}{2} \ .$$

Further, one easily checks that $e_1(\underline{\ell}) \geq s-(p-s) = p-2e_0(\underline{\ell}) \geq 3$: starting from the partition $(1,\dots,1)$, one has to move $p-s$ parts to get a partition of length s. Consider the sum $S_0 = 0\times\ell_0 + 1\times\ell_1 + \cdots + (s-1)\ell_{s-1}$. Each of the ℓ_i equals 1 when $s-e_1 \leq i \leq s-1$, hence replacing the coefficient i of ℓ_i in S_0 by $a_i = i+1$ for the last t ($\leq e_1$) values of i changes S_0 to $S_t = S_0 + t$. This can be done for any $t \in \{0,\dots,e_1\}$. If $t>0$, the largest coefficient in S_t is $a_{s-1} = s$, hence $\leq p-2$, so we may perform the operation again without any collision among coefficients modulo p, at most $p-1-(s-1) = e_0$ times. Hence we are able to transform S_0 into a sum S taking any integer value between S_0 and $S_0 + e_0e_1$ (included), with distinct coefficients mod p.

From the above, we know that $e_0e_1 \geq pe_0 - 2e_0^2$; when $p \geq 11$, one easily shows under our assumption that e_0 lies in the interval where the trinomial $-2e_0^2 + pe_0 - p$ is positive. Hence for $p \geq 11$, S can be chosen congruent to 0 mod p, with distinct coefficients $a_i \mod p$ as required. The result is easily checked for $p \in \{5,7\}$. □

The proof of (ii) ⇒ (i) is almost finished. Assuming $m(\underline{\ell}) \leq p-3$, the Lemma shows the existence of $\sigma \in \mathfrak{S}$ such that $p \mid S(\sigma(\underline{\ell})) = \sum_{i=0}^{p-1} i\ell_{\sigma(i)}$, taking σ such that $\sigma^{-1}(i) = a_i$ for $0 \leq i \leq s-1$ (since $\ell_s = \cdots = \ell_{p-1} = 0$). Since the parts ℓ_i are not all equal (otherwise $m(\underline{\ell}) = p$), let j,k be such that $\ell_{\sigma(j)} \neq \ell_{\sigma(k)}$ and let $\tau \in \mathfrak{S}$ be the product of σ with the transposition (j,k). Then

$$\sum_{i=0}^{p-1} i\ell_{\tau(i)} = \sum_{i=0}^{p-1} i\ell_{\sigma(i)} + (j-k)\big(\ell_{\sigma(k)} - \ell_{\sigma(j)}\big) \not\equiv 0 \mod p \ ,$$

since $\ell_{\sigma(k)} - \ell_{\sigma(j)} \equiv 0 \mod p$ can only occur when $\underline{\ell} = (p,0,\dots,0)$, which contradicts our hypothesis. This ends the proof of the Theorem. □

Remark. The two parts of the proof of Lemma 3.2, which is the heart of the proof of the Theorem, correspond to two different kinds of partitions: the first case ($s \leq \frac{p+1}{2}$) deals with partitions of *small length*, hence there are not too many distinct coefficients to find compared to the number of possibilities, whereas the second case deals with partitions of *large length*, in which case we use the fact that a large number of parts equal 1. Thus the proof is entirely different in the two cases, and one may wonder whether there exists a unifying proof.

The author is not able to give one at the moment. Instead, we shall give in the next section one more characterization of partitions satisfying

condition (1) or, almost equivalently, satisfying the conclusion of Lemma 3.2. It involves a larger family of partitions.

4. Around the main result: "derived" partitions

As we have noticed above, given a partition $\underline{\mathcal{L}}$ of p which is distinct from $(p, 0, \dots, 0)$, the associated p-uple $\underline{e}(\underline{\mathcal{L}}) = \big(e_0(\underline{\mathcal{L}}), \dots, e_{p-1}(\underline{\mathcal{L}})\big)$ is a composition of p. Consider the sum $S(\underline{e}(\underline{\mathcal{L}}))$: in $\sum_{k=0}^{p-1} k e_k(\underline{\mathcal{L}})$, each integer k appears $e_k(\underline{\mathcal{L}})$ times as in $\underline{\mathcal{L}}$, hence

$$\sum_{k=0}^{p-1} k e_k(\underline{\mathcal{L}}) = \sum_{i=0}^{p-1} \mathcal{L}_i = p \ .$$

Consequently, the conclusion of Lemma 3.2 becomes obvious for $\underline{\ell}$ if there exists a partition $\underline{\mathcal{L}}$ of p distinct from $(p, 0, \dots, 0)$ such that $\underline{\ell}$ is the partition in the coset of $\underline{e}(\underline{\mathcal{L}})$.

Let us say that $\underline{\ell}$ *derives from* $\underline{\mathcal{L}}$ in this situation, that is when there exists $\sigma \in \mathfrak{S}$ such that $\sigma(\underline{\ell}) = \underline{e}(\underline{\mathcal{L}})$. More precisely, one has the following equivalence.

Lemma 4.1. *A partition $\underline{\ell}$ of p derives from a partition of p if and only if there exists $\sigma \in \mathfrak{S}$ such that $S(\sigma(\underline{\ell})) = p$.*

Proof. If $\underline{\ell}$ derives from $\underline{\mathcal{L}}$, let $\sigma \in \mathfrak{S}$ be such that $\sigma(\underline{\ell}) = \underline{e}(\underline{\mathcal{L}})$, then $S(\sigma(\underline{\ell})) = p$. If $S(\sigma(\underline{\ell})) = p$ for some $\sigma \in \mathfrak{S}$, let

$$\underline{\mathcal{L}} = (p-1, \dots, p-1, p-2, \dots, p-2, \quad \dots \quad , 1, \dots, 1, 0, \dots, 0) \ ,$$

where each $0 \leq i \leq p-1$ appears $\ell_{\sigma(i)}$ times. One easily checks that $\underline{\mathcal{L}} \in \mathcal{P}$, and that $\underline{\ell}$ derives from it. □

For instance, the partition $(5, 1, 1, 0, \dots, 0)$ of 7 derives from $(4, 3, 0, \dots, 0)$, for which $e_0 = 5$ and $e_3 = e_4 = 1$, hence we get that $0{\times}5{+}3{\times}1{+}4{\times}1 = 7$; the conclusion of Lemma 3.2 is true for the partitions $(p, 0, \dots, 0)$ and $(1, \dots, 1)$ (even though the assumptions are not), and the first one is derived from the second. But, except if $p = 3$, there is no partition of p from which $(1, \dots, 1)$ would derive. More generally we show the following criterium.

Lemma 4.2. *Assume $p > 3$ and $\underline{\ell}$ derives from a partition of p, then the length s of $\underline{\ell}$ satisfies:*

$$s \leq \frac{1 + \sqrt{8p-7}}{2} \ .$$

This implies in particular $s \leq \frac{p-1}{2}$ when $p \geq 11$.

Proof. By Lemma 4.1, there exists a permutation $\sigma \in \mathfrak{S}$ such that $S(\sigma(\underline{\ell})) = p$, hence $\sum_{i=0}^{p-1} \sigma^{-1}(i)\ell_i = p$; in other words there exist s distinct numbers $a_i \in \{0, \dots, p-1\}$ such that

$$\sum_{i=0}^{s-1} a_i \ell_i = p \ .$$

The smallest sum $\sum_{i=0}^{s-1} a_i \ell_i$ with distinct coefficients $a_i \in \{0, \dots, p-1\}$ is obtained when choosing $a_i = i$ for all i, namely when affecting the biggest parts

with the smallest coefficients. Further, since $(1,\dots,1)$ and $(2,1,\dots,1,0)$ do not derive from any partition of p (here $p\neq 3$), one has $e_1(\underline{\ell})\leq s-2$ hence

$$\sum_{i=0}^{s-1} a_i\ell_i \geq \sum_{i=1}^{s-1} i\ell_i \geq 2+\sum_{i=2}^{s-1} i = 1+\frac{s(s-1)}{2} \ ,$$

which is larger than p when $s>\frac{1+\sqrt{8p-7}}{2}$. □

The condition on the length given in the Lemma is not a sufficient one, even when adding the obvious condition $s\neq 2$: for $p=7$, it yields $s\leq 4$, but $(2,2,2,1,0,0,0)$ is not derived from any partition of 7. Nevertheless, it is optimal since $(3,2,1,1,0,0,0)$ is derived from itself (analogous examples may be found for $p=11$).

Even so, the conclusion of Lemma 3.2 is true for $(2,2,2,1,0,0,0)$ as well as for $(1,\dots,1)$, hence there are in both cases distinct numbers a_i such that p divides $\sum_{i=0}^{s-1} a_i\ell_i$. Let $\sigma\in\mathfrak{S}$ be such that $\sigma^{-1}(i)=a_i$ for $0\leq i\leq s-1$, we get $p\mid S(\sigma(\underline{\ell}))$, and we may build a non increasing p-uple $\underline{\mathcal{L}}$ as in the proof of Lemma 4.1. The difference is that the sum of the parts of $\underline{\mathcal{L}}$ is now divisible by p, but not necessarily equal to p.

Define a *partition of a multiple of p with p parts* to be a p-uple of non negative integers $(\mathcal{L}_0,\dots,\mathcal{L}_{p-1})$ such that $\mathcal{L}_0\geq\mathcal{L}_1\geq\cdots\geq\mathcal{L}_{p-1}$ and $\mathcal{L}_0+\mathcal{L}_1+\cdots+\mathcal{L}_{p-1}=np$ for some positive integer n. Given such an $\underline{\mathcal{L}}$, say that a partition $\underline{\ell}$ of p *derives from* $\underline{\mathcal{L}}$ if there exists $\sigma\in\mathfrak{S}$ such that

$$\sigma(\underline{\ell}) = \big(e_0(\underline{\mathcal{L}}),\dots,e_{p-1}(\underline{\mathcal{L}})\big) \ .$$

Notice that the parts of $\underline{\mathcal{L}}$ have to be all less than p for this to happen. The proof of Lemma 4.1 readily extends to show the following.

Lemma 4.3. *A partition $\underline{\ell}$ of p derives from a partition of a multiple of p if and only if there exists $\sigma\in\mathfrak{S}$ such that $p\mid S(\sigma(\underline{\ell}))$.*

For instance $(2,2,2,1,0,0,0)$ derives from the partition of 14 with 7 parts $(5,5,2,\ 1,1,0,0)$; $(1,\dots,1)$ derives from the partition of $\frac{p(p-1)}{2}$ with p parts $(p-1,p-2,\dots,1,0)$.

The study of the basic partitions and the help of the Theorem yield the following new characterization.

Corollary 4.1. *Let $\underline{\ell}$ denote a partition of p. Then the following are equivalent:*

(i) $m(\underline{\ell})\neq p-2$.
(ii) $\exists\ \sigma\in\mathfrak{S}$ *such that* $p\mid S(\sigma(\underline{\ell}))$.
(iii) $\underline{\ell}$ *is derived from a partition of a multiple of p with p parts.*

Remark. Notice that the partition $(p-2,1,1,0\dots,0)$ derives from all the partitions with maximal number of equal parts $m(\underline{\ell})=p-2$, namely $(2,1,\dots,1,0)$ and $(p-k,k,0,\dots,0)$, $1\leq k\leq\frac{p-1}{2}$. Further, replacing $\underline{e}(\underline{\ell})$ by $\underline{e}'(\underline{\ell})=(e'_0(\underline{\ell}),\dots,e'_{p-1}(\underline{\ell}))$ defined by

$$e'_k(\underline{\ell}) = \#\{0\leq i\leq p-1 \mid \ell_i\equiv k \mod p\} \ ,$$

we get an analogous characterization of the partitions such that $p\mid S(\sigma(\underline{\ell}))$ for all $\sigma\in\mathfrak{S}$, namely $(1,\dots,1)$ and $(p,0,\dots,0)$: they both satisfy $\underline{e}'(\underline{\ell})\in$

$(p, 0, \dots, 0)$ — here we see a partition as a coset of compositions. We obtain:

$$\begin{array}{ll} \exists\, \sigma \in \mathfrak{S},\ p \mid S(\sigma(\underline{\ell})) & \iff \ \underline{e}'(\underline{\ell}) \notin (p-2, 1, 1, 0 \dots, 0)\ ; \\ \exists\, \tau \in \mathfrak{S},\ p \not| \ S(\tau(\underline{\ell})) & \iff \ \underline{e}'(\underline{\ell}) \notin (p, 0 \dots, 0)\ . \end{array}$$

It follows that assertion (1) is also equivalent to:

$$\underline{e}'(\underline{\ell}) \notin (p-2, 1, 1, 0 \dots, 0) \cup (p, 0 \dots, 0)\ .$$

References

[A] Andrews G.E., *The theory of partitions*, Encyclopedia of Mathematics and its applications **2**, Addison-Wesley (1976).

[DM] Dixon J.D., Mortimer B., *Permutation groups*, Graduate Texts in Mathematics **163**, Springer-Verlag, New York (1996).

[V] Vinatier S., Galois module structure in wealky ramified 3-extensions, *Acta Arithm.* **119**, *no. 2*, 171–186 (2005).

Stéphane Vinatier
XLIM UMR 6172 CNRS / Université de Limoges
Faculté des Sciences et Techniques
123 avenue Albert Thomas
87060 Limoges Cedex, France
E-mail : stephane.vinatier@unilim.fr
URL: http://www.unilim.fr/pages_perso/stephane.vinatier/