Strictly chained (p, q)-ary partitions

Laurent Imbert

Joint work with Fabrice Philippe, Montpellier, France

CNRS, PIMS, University of Calgary

Alberta Number Theory Day – April 30, 2009

About the PIMS/CNRS agreement

The CNRS (National Center for Scientific Research) is a government-funded research organization, under the administrative authority of France's Ministry of Research.

In September 2007, PIMS has become an Unite Mixte Internationale of the CNRS. (There are only four UMIs in mathematics around the world: in Moscow, Rio, Santiago, and now PIMS.)

Under this agreement, French researchers can be sent for one year by the CNRS to a PIMS university.

Call for applications 2010 – 2011 is open (deadline: Dec. 1st, 2009)

http://www.pims.math.ca/about-us/opportunities

Outline

- Quick introduction to integer partitions
- Strictly chained (p, q)-ary partitions
  - Encoding
  - Generating
  - Counting
- Applications
- Shortest (p, q)-ary partitions
- Open problems

Integer partitions

A *partition* of an integer n is a nonincreasing sequence of positive integers $a_1, a_2, \ldots, a_k$ whose sum is n. Each a_i is called a *part*.

For example, here are the 5 partitions of the integer 4:

$$
\begin{aligned}
4 &= 4 \\
&= 3 + 1 \\
&= 2 + 2 \\
&= 2 + 1 + 1 \\
&= 1 + 1 + 1 + 1
\end{aligned}
$$

The partitions of n correspond to the set of solutions $(k_1, k_2, \ldots, k_n)$ in nonnegative integers to the Diophantine equation

$$1k_1 + 2k_2 + 3k_3 + \cdots + nk_n = n$$

Ferrers diagrams

A nice and useful way to visualize partitions:

$$
\begin{array}{rrl}
15 = & 6 & \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet \\
 & +\,3 & \bullet\ \bullet\ \bullet \\
 & +\,3 & \bullet\ \bullet\ \bullet \\
 & +\,2 & \bullet\ \bullet \\
 & +\,1 & \bullet
\end{array}
$$

$p(n,k)$: The number of partitions of n whose largest part is k is equal to the number of partitions of n with k parts.

$p(n)$: The number of (unrestricted) partitions of n, where the order is not significant ($p(n) = 0$ for all $n < 0$ and $p(0) = 1$).

$\mathcal{P}(4) = \{(4), (3,1), (2,2), (2,1,1), (1,1,1,1)\}, \quad p(4) = 5.$

Euler's partition function

Consider the product

$$(1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots \quad (1)$$

What is the coefficient of x^n in (1)?

Each contribution (of 1) to the coefficient of x^n is of the form

$$x^{1k_1} \cdot x^{2k_2} \cdot x^{3k_3} \cdots = x^{1k_1 + 2k_2 + 3k_3 + \cdots}$$

Thus, the coefficient of x^n is the number of ways of writing n as $1k_1 + 2k_2 + 3k_3 + \cdots + nk_n$, where $k_i \geq 0$. This is exactly $p(n)$.

$$\sum_{n=0}^{\infty} p(n)x^n = \frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdots = \mathcal{E}(x)$$

Example 1

Let $f(n)$ denote the number of partitions of n with no part 1.

$$\begin{aligned}\sum_{n=0}^{\infty} f(n)x^n &= x^0 \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdots \\ &= \frac{1-x}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdots \\ &= (1-x)\mathcal{E}(x)\end{aligned}$$

This generating function yields the following result:

Lemma: $f(n) = p(n) - p(n-1)$.

Bijective proof: if a partition of n contains at least one part equal to 1, then removing one of these yields a partition of $n-1$. □

Example 2

$q(n)$ is the number of partitions of n with disctinct parts.

$$\sum_{n=0}^{\infty} q(n)x^n = (1+x)(1+x^2)(1+x^3)\cdots$$
$$= \frac{1-x^2}{1-x} \cdot \frac{1-x^4}{1-x^2} \cdot \frac{1-x^6}{1-x^3} \cdot \frac{1-x^8}{1-x^4} \cdots$$
$$= \frac{1}{1-x} \cdot \frac{1}{1-x^3} \cdot \frac{1}{1-x^5} \cdots$$

Theorem: The number of partitions of n with distinct parts is equal to the number of partitions with odd parts.

Bijective proof: uses the fact that each part can be written as a power of 2 times an odd number.

More examples

- Partitions into primes (Goldbach conjecture)
- m-ary partitions: partitions as a sum of powers of m for a fixed $m \geq 2$. (e.g. binary partitions)
- Partitions with parts occurring at most thrice [A. Fink, R. Guy, M. Krusemeyer 2008]

$$(1+x+x^2+x^3)(1+x^2+x^4+x^6)(1+x^3+x^6+x^{12})\cdots$$

$=$ Partitions with no part a multiple of 4
$=$ Partitions with no even parts repeated

- Chain, umbrella partitions: partitions constrained by divisibility conditions

Chain partitions

A *(strictly) chain partition* is a partition of the form $n = a_1 + a_2 + \cdots + a_k$ into (distinct) positive integers such that $a_k | a_{k-1} | \ldots | a_2 | a_1$.

$$\begin{aligned} 873 &= 512 + 256 + 64 + 32 + 8 + 1 \\ &= 720 + 120 + 24 + 6 + 2 + 1 \\ &= 696 + 174 + 3 \end{aligned}$$

[Erdös-Loxton 1979]

- # partitions of this type: $p(n) \geq \log_2 n$ for $n \geq 6$
- # partitions of this type whose smallest part is 1: $p_1(n) \geq \frac{1}{2} \log_2 n$ for $n \geq 27$ and $n - 1$ not a prime
- $P(x) = \sum_{1 \leq n \leq x} p(n) \approx cx^{\rho}$, where c is an unknown constant and ρ is the unique root of $\zeta(s) - 2$, where ζ is the Riemann zeta function.

Strictly chained (p, q)-ary partition

Strictly chained (p, q)-ary partitions are chain partitions with distinct parts of the form $p^a q^b$, where $p, q \geq 2$ and $(p, q) = 1$.

Notations:

- $\Omega(U)$: The set of all strictly chained (p, q)-ary partitions of U
- $\Omega^*(U)$: The subset of partitions $\omega \in \Omega(U)$ with no part 1
- $W(U) = \#\Omega(U)$
- $W^*(U) = \#\Omega^*(U)$

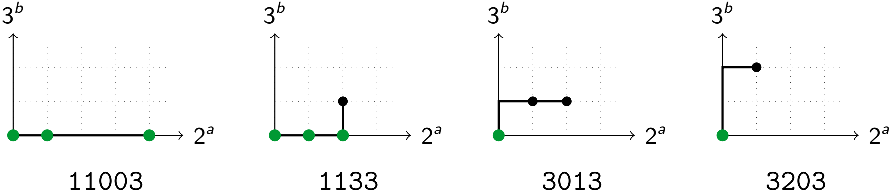
Special cases of interest:

- $\min(p, q) = 2$
- $(p, q) = (2, 3)$

Graphic representation and encoding

Example with $(p, q) = (2, 3)$.

$\Omega(19) = \{(16, 2, 1), (12, 4, 2, 1), (12, 6, 1), (18, 1)\}$



The couples of exponents (a, b) form a chain in $\mathbb{N}^2$. They can be encoded with words in $\{0, 1, 2, 3\}^*$. (Conventions: words end with '3', we go North before going East) If $\min(p, q) = 2$, the *binary amount* of a partition is equal to the sum of all its binary parts (● parts) or 0 if none.

Complete generation, maps

We define embeddings from subsets $\Omega \subset \Omega(U)$ to $\mathcal{P}$, the set of all unrestricted partitions (sequences of positive integers whose sum is finite)

Let $\omega = (a_1, a_2, \ldots, a_k) \in \Omega$.

- Mult. by p: $\omega \longmapsto (pa_1, pa_2, \ldots, pa_k) \in {}^p\Omega$
- Mult. by q: $\omega \longmapsto (qa_1, qa_2, \ldots, qa_k) \in {}^q\Omega$
- Add. 1: $\omega \longmapsto \begin{cases} (a_1, \ldots, a_k, 1) & \text{if } \min(p,q) > 2 \\ \text{binary amount} + 1 & \text{if } \min(p,q) = 2 \end{cases}$

  In both cases, the resulting set of partitions is denoted ${}^1\Omega$.

  Remark: the number of parts never increases by more than 1 and may be reduced due to carry propagation.

Complete generation, maps' properties

- ${}^{p}\Omega(U) \subset \Omega(pU)$
- ${}^{q}\Omega(U) \subset \Omega(qU)$
- ${}^{1}\Omega(U) \not\subset \Omega(U+1)$ in general

  If $\min(p, q) > 2$, the part 1 may appear twice in ${}^{1}\Omega$

  The strictly chained $(2, 3)$-ary partition $(6, 2, 1)$ is turned into $(6, 4) \notin \Omega(10)$

- If $\min(p, q) = 2$, the set $\Omega(U)$ contains at least the binary partition of U.
- By convention $\Omega(0) = \{()\}$

Some formulæ

Lemma: (+ denotes union of disjoint sets)

$$\Omega(U) = \Omega^*(U) + {}^1\Omega^*(U-1), \qquad \Omega^*(U) = {}^p\Omega(U/p) \cup {}^q\Omega(U/q)$$

Corollary:

$$\Omega(pqU) = {}^p\Omega(qU) + {}^q(\Omega(pU) \setminus {}^p\Omega(U)),$$
$$\Omega(pqU+1) = {}^{1p}\Omega(qU) + {}^{1q}(\Omega(pU) \setminus {}^p\Omega(U))$$

and for $1 < r < pq$

$$\Omega(pqU + r) = \Omega^*(pqU + r) + {}^1\Omega^*(pqU + r - 1) \tag{2}$$

Both sets Ω^* in the rhs of (2) are non empty if and only if:
$r = kp$ and $r - 1 = \ell q$, or $r = \ell q$ and $r - 1 = kp$.

Let $k_0 = p^{-1} \bmod q$ and $\ell_0 = q^{-1} \bmod p$. Then, $(k_0, p - \ell_0)$ is the unique positive solution to the equation $kp - \ell q = 1$. Therefore:

$$\text{if } r = k_0 p, \quad \Omega(pqU + r) = {}^p\Omega(qU + k_0) + {}^{1q}\Omega(pU + p - \ell_0)$$

Simpler relations

The complete formula:

$$\Omega(pqU+r) = \begin{cases} {}^{p}\Omega(qU+k_0) + {}^{1q}\Omega(pU+p-\ell_0) & \text{if } r = k_0 p \\ {}^{q}\Omega(pU+\ell_0) + {}^{1p}\Omega(qU+q-k_0) & \text{if } r = \ell_0 q \\ {}^{p}\Omega(qU+k) & \text{if } r = kp,\ k \neq k_0 \\ {}^{1p}\Omega(qU+k) & \text{if } r = kp+1,\ k \neq q-k_0 \\ {}^{q}\Omega(pU+\ell) & \text{if } r = \ell q,\ \ell \neq \ell_0 \\ {}^{1q}\Omega(pU+\ell) & \text{if } r = \ell q+1,\ \ell \neq p-\ell_0 \\ \emptyset & \text{otherwise.} \end{cases}$$

The case $(p,q) = (2,3)$ allows for some simplifications:

$$\begin{aligned} \Omega(3U) &= {}^{3}\Omega(U) + {}^{1}\Omega(3U-1) \\ \Omega(6U-1) &= {}^{12}\Omega(3U-1) \\ \Omega(6U+1) &= {}^{13}\Omega(2U) + {}^{11}\Omega(6U-1) \\ \Omega(6U+2) &= {}^{2}\Omega(3U+1) \\ \Omega(6U+4) &= {}^{13}\Omega(2U+1) + {}^{2}\Omega(3U+2) \end{aligned}$$

Examples

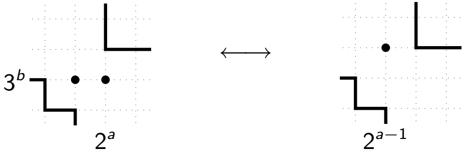
$$\Omega(217) = \{3000133,\ 30001003,\ 322033,\ 3220003,\\ 3200013,\ 10011013,\ 1001333,\ 10013003\}$$

$$\Omega(95) = \{1111103\}$$
$$\Omega(6143) = \{1111111111103\}$$

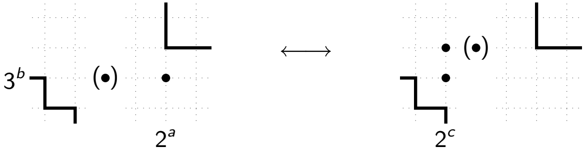
$$\Omega(575) = \{1111110003,\ 111111033\}$$
$$\Omega(959) = \{1111110113,\ 1111110303\}$$

Transitions

- $1 + 2 = 3$



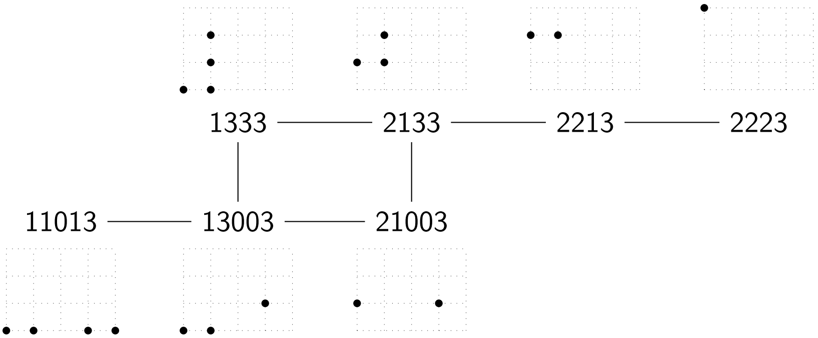
- $2(2^m - 1 + 2^{m+1}) = 3(2^{m+1} - 1) + 1$ (generalizes $4 = 3 + 1$)



Random walk

The transition graph is symmetric and connected.

E.g: $G(27)$ for $(p, q) = (2, 3)$



Computing $W(U)$

Let $W_p(U) \in \{0,1\}$ be the number of partitions of U with distinct parts taken in $\{p^n, n \in \mathbb{N}\}$. In other words, can U be written in base p with digits $\{0,1\}$ only?

$$W(U) = W_p(U) + W\left(\frac{U}{q}\right) + \sum_{c=0}^{\left\lfloor \log_p\left(\frac{U}{q+1}\right)\right\rfloor} \delta_{p,q}(c,U)\, W\left(\left\lfloor \frac{U}{p^c q}\right\rfloor\right),$$

$$\delta_{p,q}(c,U) = \begin{cases} 1 & \text{if } \lfloor U/p^c \rfloor \equiv 1 \pmod{q} \text{ and } W_p(U \bmod p^c) = 1 \\ 0 & \text{otherwise} \end{cases}$$

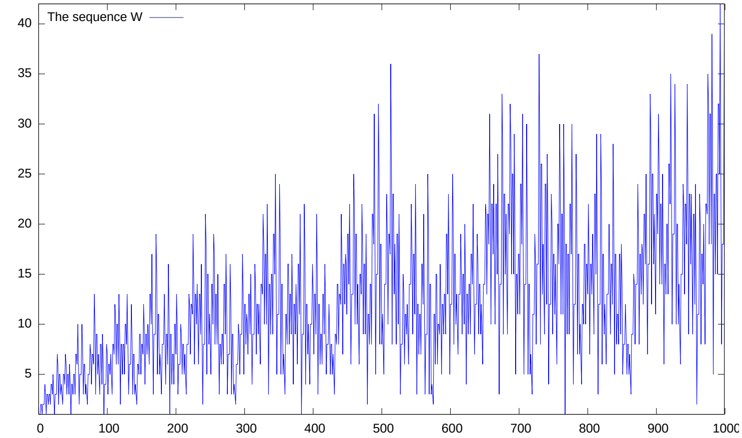
Sketch of proof: Order the partitions in $\Omega(U)$ w.r.t p-ary amount

$$W(U) = W(U/q) + \sum_{n=1}^{U} W_p(n)\, W\left(\frac{U-n}{p^{c_n} q}\right).$$

and remark that many summands vanish.

The sequence W

For any pair (p, q), the sequence W behaves rather irregularly.



Properties of W

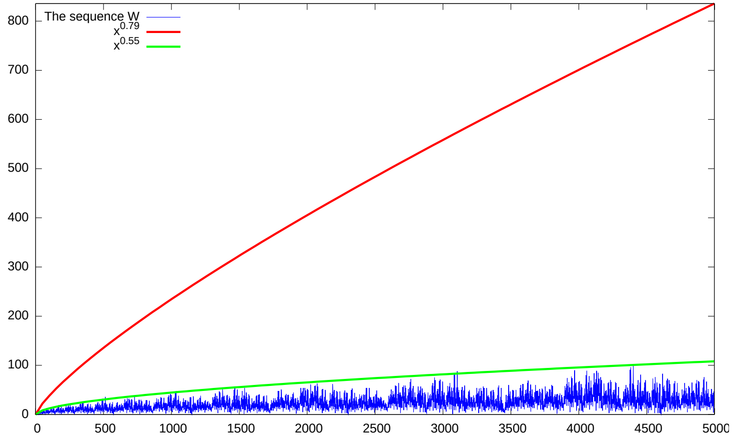
- W takes infinitely often the value 0
- If $\min(p, q) = 2$, then W takes infinitely often the value 1
- If $(p, q) = (2, 3)$, we have $W(U) = 1$ iff either $U \in \{0, 1\}$ of $U = 2^a 3 - 1$ for some $a \in \mathbb{N}$. Also, $W(U) = 2$ iff either $U \in \{3, 5, 6, 7\}$ or $U = 2^a 9 - 1$ or $U = 2^a 15 - 1$ for some $a \in \mathbb{N}$.

  Conjecture: all values in $\mathbb{N}$ are taken
- Theorem: The sequence W is either $\{0, 1\}$-valued or unbounded.

  Note: We are not aware of any pair (p, q) for which W is $\{0, 1\}$-valued.

Asymptotical behaviour of max W

Max value: Let $\beta \in (0,1)$ be the unique solution of $1/p^\beta + 1/q^\beta = 1$. Then $W(U) \leq U^\beta$ for $U \geq 1$. For $(p,q) = (2,3)$, we can (only) prove $W(U) \leq U^{0.79}$, whereas our numerical experiment suggest $U^{0.55}$.



Average value of W

Let $S(x) = \sum_{1 \leq U \leq \lfloor x \rfloor} W(U)$.

$$S(x) = \sum_{U=1}^{\lfloor x \rfloor} (W^*(U) + W^*(U-1))$$

$$= W^*(0) - W^*(\lfloor x \rfloor) + 2 \sum_{U=1}^{\lfloor x \rfloor} (W(U/p) + W(U/q) - W(U/pq))$$

Then, for all $x \in \mathbb{R}^+$ we have

$$S(x) = 2(S(x/p) + S(x/q) - S(x/pq)) + 1 - W^*(\lfloor x \rfloor)$$

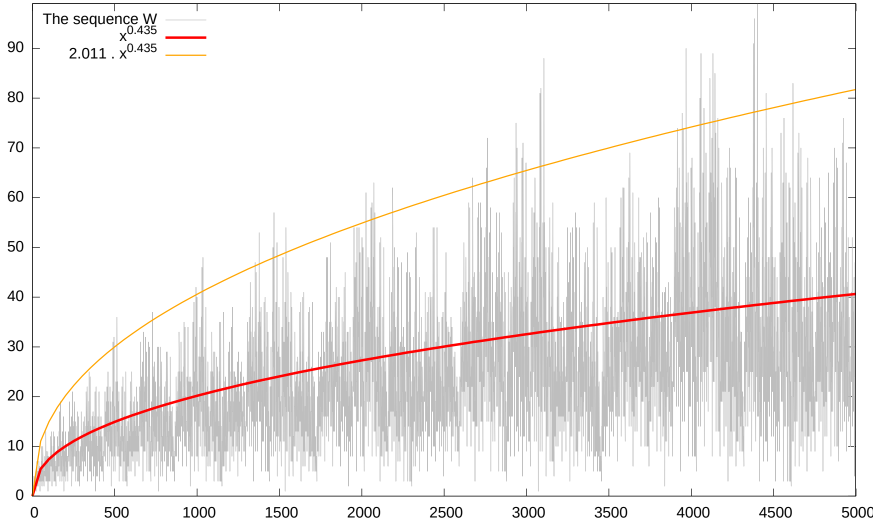
Therefore, if $S(x) \approx x^\alpha$, then α satisfies

$$1/p^\alpha + 1/q^\alpha - 1/(pq)^\alpha = 1/2$$

which also reads

$$(1 - p^{-\alpha})^{-1}(1 - q^{-\alpha})^{-1} = 2$$

Average value of W

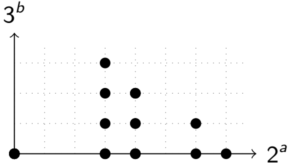


Applications

Fast exponentiation: given $g \in G$ and $e \geq 0$ compute g^e

$$g^{217} = (((g^2 \times g)^{2^2} \times g)^2 \times g)^{2^{2^2}} \times g$$

cost: 4 mults, 7 squares



$$g^{217} = g^{2^{2^{2^{3^{3^3}}}}} \times g$$

cost: 1 mult, 3 squares, 3 cubes

Requires: fast cubing (e.g. elliptic curves, quadratic fields), and a fast conversion algorithms into strictly chained $(2,3)$-ary partitions.

Conversion algorithms

- Right-to-left: divide by 3 and by 2 as much as possible; add or subtract 1 to make the resulting value divisible by 3

- Left-to-right: find the closest number of the form $2^a 3^b$ from e; subtract and continue until reaching 0

- None of these algorithm give a chain of minimal length.

- Can we find a shortest partition, or at least, compute its length?

Shortest partitions

Let $|w|$ the number of parts of a partition $w \in \Omega(U)$. We define $\sigma(U) = \min_{w \in \Omega(U)} |w|$, the length of a shortest partition in $\Omega(U)$.

$$\Omega(pqU) = {}^{p}\Omega(qU) + {}^{q}(\Omega(pU) \setminus {}^{p}\Omega(U)),$$
$$\Omega(pqU+1) = {}^{1p}\Omega(qU) + {}^{1q}(\Omega(pU) \setminus {}^{p}\Omega(U))$$

The mappings ${}^{p}\Omega$ and ${}^{q}\Omega$ do not change the number of parts.

$$\sigma(pqU) = \min(\sigma(qU), \sigma(pU))$$
$$\sigma(pqU+1) = 1 + \sigma(pqU)$$

Similarly, the relations in (2) can be adapted for numbers of the form $pqU + r$ for $1 < r < pq$.

Computing shortest partitions

For $(p, q) = (2, 3)$ the following Maple code can be used to compute the first 500000 values of σ in approximately 1 second.

```
s := proc(U)
option remember;
local r;
if U <= 2 then 1 else
r := irem(U,6);
if r=0 then min(s(U/3), s(U/2))
elif r=1 then 1 + s(U-1)
elif r=2 then s(U/2)
elif r=3 then min(s(U/3), 1+s((U-1)/2))
elif r=4 then min(s(U/2), 1+s((U-1)/3))
elif r=5 then 1 + s((U-1)/2)
fi: fi: end:
```

Remark: numercal experiments suggest $\sigma(U) \approx (\log_2 U)/4$ on average

Open questions

- When computing g^{-1} in G is easy, one may want to consider signed chained partitions, where the largest part in w is less than $f(U)$ for some function f (e.g $f(U) = U + 1$), while allowing the other parts to be either added or subtracted.

  Example: $314159 = \dots$
  Right-to-left: [1,9,6][-1,8,5][1,7,3][-1,5,2][-1,4,1][-1,0,0]
  Left-to-right: [1,4,9][-1,0,6][-1,0,3][-1,0,2][-1,0,1][-1,0,0]

  - Generating, random walk, etc?
  - How many are there?
  - Shortest signed partition?
  - Optimal choice of f?

- Many other questions related to numbers composed of small primes (density of various sequences)

Thanks!

http://www.lirmm.fr/~imbert