How to compute shortest double-base chains?

Laurent Imbert and Fabrice Philippe, CNRS-LIRMM, Montpellier, France

Motivations and Introduction

This work arose from recent developments on double-base representations, in particular their use in speeding-up elliptic curve scalar multiplication [1]. In this system, a positive integer is written as a sum of terms of the form $p^a q^b$ for two pairwise prime integers p, q. Here, we concentrate on the case $(p, q) = (2, 3)$.

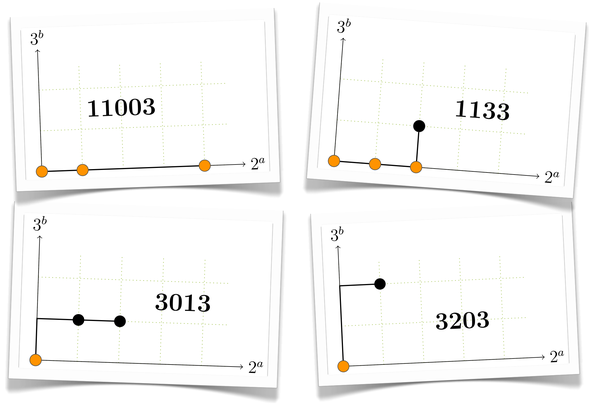
Double-base chains can be seen as strictly chained {2,3}-ary partitions ; *i.e.* partitions of the form $n = a_1 + a_2 + \cdots + a_k$ into distinct positive parts $a_1, a_2, \ldots, a_k$ of the form $2^a 3^b$ with $a, b \geq 0$, and such that each part is a multiple of the following one:

$$361 = 2^2 3^4 + 2^2 3^2 + 2^0 3^0 = 324 + 36 + 1$$

Partitions into which parts are restricted by divisibility conditions have already been studied by Erdös and Loxton in [2].

Visualization and Encoding

Those partitions can be visualized with 2D graphs, where the point (a, b) corresponds to the summand $2^a 3^b$. The graphs below represent the 4 strictly chained {2,3}-ary partitions of 19: {(16, 2, 1), (12, 4, 2, 1), (12, 6, 1), (18, 1)}.



They can be encoded with words on $\{0, 1, 2, 3\}$. The binary amount is the sum of all the binary parts (orange dots) or 0 if none.

Complete Generation

Let $\Omega(U)$ denote the set of all strictly chained {2,3}-ary partitions of U, and $\Omega^*(U)$ its subset of partitions $\varpi \in \Omega(U)$ with no part 1. We define three mappings from subsets Ω of $\Omega(U)$ to the set $\mathcal{P}$ of all (general) partitions.

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

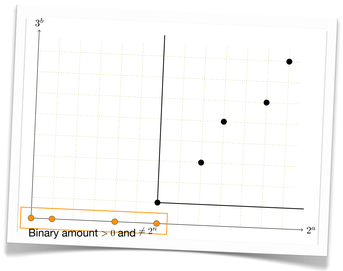
${}^2\Omega : \varpi \mapsto (2a_1, 2a_2, \ldots, 2a_k)$	mult by 2
${}^3\Omega : \varpi \mapsto (3a_1, 3a_2, \ldots, 3a_k)$	mult by 3
${}^1\Omega : \varpi \mapsto (a'_1, a'_2, \ldots, a'_l)$	increment binary amount

Partitions in $\Omega(U)$ can be computed recursively by considering partitions with or without part 1 and by noticing that, in a partition with no part 1, either 2 or 3 (or both) must divide all parts. We have $\Omega(1) = \{(1)\}$ and for any integer $U > 0$

$$(1) \qquad \Omega(U) = \Omega^*(U) + {}^1\Omega^*(U-1)$$
$$(2) \qquad \Omega^*(U) = {}^2\Omega(U/2) \cup {}^3\Omega(U/3)$$

In general, relation (2) involve set difference but it can be simplified when $\min(p, q) = 2$.

$$\begin{aligned}\Omega(3U) &= {}^3\Omega(U) + \Omega(3U) \backslash {}^3\Omega(U) \\ &= {}^3\Omega(U) + {}^1\Omega(3U-1)\end{aligned}$$



In some well defined cases, both sets in (1) are non empty, *e.g.*

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

In the other cases only one of them do contribute.

$$\Omega(6U+5) = {}^{12}\Omega(3U+2)$$
$$\Omega(6U+2) = {}^2\Omega(3U+1)$$

Shortest Partitions

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

```
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)
  end if
end if
end:
```

The equations for Ω can be adapted to compute values of σ, in particular by noticing that ${}^2\Omega$ and ${}^3\Omega$ do not increase the number of parts of a partition.

The recursive function above can be used to compute values of σ quite efficiently. It can be adapted to return a partition of length $\sigma(U)$.

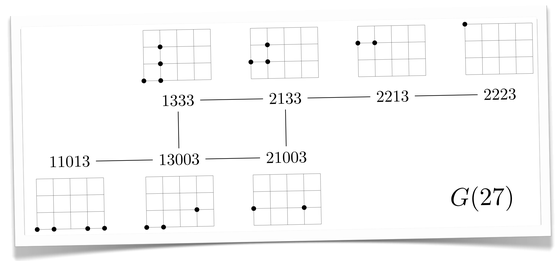
Example: $\sigma(17^{71}) = 78$.

1000320320100032001000010033323000322322003200100003201000100010100110100030000000010001100010010000000030032200332221032010300033223320333220332103232221000321010000000303000000301010110010010000110030100003200321030003201010003000000000300320100003

Our numerical experiments suggest that $\sigma(U) \simeq (\log_2 U)/4$ on average. It is perhaps possible to significantly reduce the minimum number of parts, for example by allowing negative parts. Studying similar relaxed definitions of chained partitions is the object of further research.

More...

There exists a symmetric, connected transition graph on $\Omega(U)$.



Let $W(U) = \#\Omega(U)$. The sequence W behaves quite irregularly and several questions remain open. For example, one can prove that it is either $\{0, 1\}$-valued or unbounded but we have not been able to find a pair (p, q) for which it is $\{0, 1\}$-valued. Also, our numerical experiments suggest that all values in $\mathbb{N}$ are taken infinitely many times by W, but this remains to be proved.

References

[1] V. Dimitrov, L. Imbert and P. K. Mishra. The Double-base Number System and its Application to Elliptic Curve Cryptography, Math. Comp., 77(2), pp 1075–1104, 2008. (see also the ASIACRYPT 2005 and INDOCRYPT 2006 papers)

[2] P. Erdös and J. H. Loxton. Some Problems in Partitio Numerorum, Journal of the Australian Mathematical Society, Series A 27 (1979), no 3, 319–331.

[3] L. Imbert and F. Philippe. Strictly Chained (p,q)-ary Partitions. Contributions to Discrete Mathematics, 2010 (to appear).

LIRMM

cnrs