



s-partitions

William M.Y. Goh, Paweł Hitczenko*, Ali Shokoufandeh

Department of Mathematics and Computer Science, Drexel University, Philadelphia, PA 19104, USA

Received 1 December 2000; received in revised form 1 July 2001

Communicated by S.E. Hambrusch

Abstract

This note reports on the number of *s*-partitions of a natural number n . In an *s*-partition of n each cell has the form $2^k - 1$ for some integer k . Such partitions have potential applications in cryptography, specifically in distributed computations of the form $a^n \bmod m$. The main contribution of this paper is a correction to the upper bound on number of *s*-partitions presented by Bhatt [Inform. Process. Lett. 71 (1999) 141–148]. We will give a precise asymptotics for the number of such partitions for a given integer n . © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Combinatorial problems; Integer partitions

1. Introduction

The *s*-partition of an integer n is a decomposition $n = \sum_i n_i$ such that each n_i is of the form $2^k - 1$, for some integer k . Closely related are *binary partitions*, i.e., partitions whose cells are powers of 2 (see [2]). Perhaps, the simplest form of a binary partition of a number is its binary representation, in which each part size has the form 2^k , for some integer k . Given an integer n its binary representation can be computed by using consecutive shifts in $\Theta(\log n)$ steps.

An important computation in most of the cryptographic systems is the computations of the form $a^n \bmod m$ (see [3]). In [1], Bhatt presented an NC-algorithm for computations of this form on a CRCW parallel model. While giving a characterization of *s*-partitions, for a given integer n , he presented a simple

algorithm for computing its *d*-partition in $\Theta(\log n)$. He went on to use this decomposition in computing $a^n \bmod m$ in poly-logarithmic time on a distributed system, using polynomial number of processors in terms of n .

As the main theoretical result Bhatt gave the quantity

$$2 + \left\lfloor \frac{n}{3} \right\rfloor + \sum_{i=0}^{\lfloor \log n \rfloor} \lfloor \log(n - 3i) \rfloor^{\lfloor \log(n-3i) \rfloor - 1},$$

(where \log means \log_2) as an upper bound for the number of *s*-partitions of an integer n , but this bound is not correct. The purpose of this note is to present a correction to his result by giving a precise asymptotics for the number of *s*-partitions. Specifically, we have

Theorem 1. *Let $p_s(n)$ denote the total number of *s*-partitions of an integer n and for a function*

$$f(x) = \left\lfloor \frac{\ln x}{\ln 2} \right\rfloor - \frac{\ln x}{\ln 2} + \frac{1}{2},$$

* Corresponding author.

E-mail addresses: wgo@mcsc.drexel.edu (W.M.Y. Goh),
phitczen@mcsc.drexel.edu (P. Hitczenko),
ashokouf@mcsc.drexel.edu (A. Shokoufandeh).

let

$$\alpha := \lim_{u \rightarrow \infty} \int_2^u \frac{f(v)}{v(v-1)} dv = -0.4934 \dots$$

Then,

$$\begin{aligned} \ln p_s(n) &= \frac{1}{2 \ln 2} (\ln(n+1) - \ln \ln(n+1) + \ln \ln 2)^2 \\ &\quad + \left(\frac{1}{\ln 2} - \frac{3}{2} \right) \ln(n+1) + \ln \ln(n+1) - \ln \ln 2 \\ &\quad + W(\ln(n+1) - \ln \ln(n+1) - \ln \ln 2) \\ &\quad - \frac{1}{2} \ln 2\pi + H + o(1), \end{aligned}$$

where

$$H = \frac{\pi^2 + \ln^2 2}{12 \ln 2} + \alpha + \frac{1}{\ln 2} \int_0^\infty \frac{\ln v - \ln(1 - e^{-v})}{e^v - 1} dv,$$

and

$$\begin{aligned} W(z) &= - \sum_{v \neq 0} \left(\frac{2\pi v}{\ln 2} \right)^2 \Gamma \left(\frac{2\pi i v}{\ln 2} \right) \\ &\quad \times \zeta \left(1 + \frac{2\pi i v}{\ln 2} \right) c_v e^{(2\pi i v / \ln 2)z}. \end{aligned}$$

A proof is a quick consequence of a theorem that was proven with binary partitions in mind. Such partitions have been studied by several authors beginning in the 40's. Not surprisingly, the results obtained by these authors are general enough to be applicable in the context of s -partitions. We will recall one such theorem proved in [2] in the next section.

2. Proof of Theorem 1

Here is a relevant part of a theorem proved by Pennington. We refer the reader to his paper [2] for more details and credits concerning pre-1953 activities.

Theorem 2. Let $0 < \lambda_1 < \lambda_2 < \dots$ be a given sequence of numbers with

$$N(u) = \sum_{\lambda_v \leq u} 1 = a \ln u + b + R(u)$$

for $u > 0$, where

$$\int_{\lambda_1}^u \frac{R(v)}{v} dv = c + V \left(\frac{\ln u}{\rho} \right) + o(1)$$

as $u \rightarrow \infty$, a, b, c, ρ are constants, $a > 0, \rho > 0$, and V is a periodic function with period 1, bounded and integrable in the interval $0 \leq x \leq 1$. Let $\{c_v: -\infty < v < \infty\}$ be the complex Fourier coefficients of V and suppose that $c_0 = 0$ and $\sum_{v \neq 0} |c_v/v| < \infty$. For real u let $P(u)$ be the number of solutions of the inequality

$$r_1 \lambda_1 + r_2 \lambda_2 + r_3 \lambda_3 + \dots < u$$

in integers $r_v \geq 0$, and let

$$P_h(u) = \{P(u) - P(u-h)\} / h.$$

Then, if h is a positive constant for which $P_h(u)$ is an increasing function of u (this condition is certainly satisfied if h belongs to the sequence λ_v), as $u \rightarrow \infty$,

$$\begin{aligned} \ln P_h(u) &= \frac{1}{2} a (\ln u - \ln \ln u - \ln a)^2 + \left(a - \frac{1}{2} \right) \ln u \\ &\quad + \left(b - \frac{1}{2} \right) (\ln u - \ln \ln u - \ln a) \\ &\quad + W(\ln u - \ln \ln u - \ln a) \\ &\quad - \frac{1}{2} \ln 2\pi + H + o(1), \end{aligned}$$

where

$$\begin{aligned} H &= c - b \ln \lambda_1 - \frac{1}{2} a \ln^2 \lambda_1 \\ &\quad + a \int_0^\infty \frac{\ln v - \ln(1 - e^{-v})}{e^v - 1} dv, \end{aligned}$$

and

$$\begin{aligned} W(z) &= - \sum_{v \neq 0} \left(\frac{2\pi v}{\rho} \right)^2 \Gamma \left(\frac{2\pi i v}{\rho} \right) \\ &\quad \times \zeta \left(1 + \frac{2\pi i v}{\rho} \right) c_v e^{(2\pi i v / \rho)z}. \end{aligned}$$

The function $W(z)$ is defined for all $z = x + iy$ in the strip $|y| < \frac{1}{2}\pi$, and is bounded and uniformly continuous in any fixed interior strip $|y| \leq M < \frac{1}{2}\pi$.

We observe that if $\lambda_1 = 1$ then, for an integer n , $P_1(n+1)$ counts the number of partitions of n into parts of sizes in the set $\{\lambda_v: v \geq 1\}$. In particular, $p_s(n) = P_1(n+1)$ for the sequence $\lambda_v = 2^v - 1, v \geq 1$. Thus, in order to prove Theorem 1, it suffices

to check that this sequence satisfies the assumptions of Pennington’s theorem with

$$\begin{aligned}
 a &= \frac{1}{\ln 2}, \quad b = -\frac{1}{2}, \\
 c &= \frac{\pi^2 + \ln^2 2}{12 \ln 2} + \alpha, \quad \rho = \ln 2.
 \end{aligned}
 \tag{1}$$

To this end we write

$$\begin{aligned}
 N(u) &= \sum_{\substack{2^v \leq u+1 \\ v \geq 1}} 1 = \left\lfloor \frac{\ln(u+1)}{\ln 2} \right\rfloor \\
 &:= \frac{\ln u}{\ln 2} - \frac{1}{2} + R(u),
 \end{aligned}
 \tag{2}$$

and we will show that

$$\begin{aligned}
 R(u) &:= \frac{\ln(1 + 1/u)}{\ln 2} \\
 &\quad + \left(\left\lfloor \frac{\ln(u+1)}{\ln 2} \right\rfloor - \frac{\ln(u+1)}{\ln 2} + \frac{1}{2} \right)
 \end{aligned}$$

has the desired properties. Since $\lambda_1 = 1$, we have

$$\int_{\lambda_1}^u \frac{R(v)}{v} dv = \int_1^u \frac{\ln(1 + 1/v)}{\ln 2} \frac{dv}{v} + \int_1^u \frac{f(v+1)}{v} dv,
 \tag{3}$$

where

$$f(x) = \left\lfloor \frac{\ln x}{\ln 2} \right\rfloor - \frac{\ln x}{\ln 2} + \frac{1}{2}$$

as defined in Theorem 1. Changing the variables $t = 1/v$ in the first integral we see that it converges to

$$\frac{1}{\ln 2} \int_0^1 \frac{\ln(1+t)}{t} dt = \frac{\pi^2}{12 \ln 2}.
 \tag{4}$$

To handle the second integral, we rely on work of Pennington who showed that

$$\int_1^u \frac{f(v)}{v} dv = \frac{\ln 2}{12} - \sum_{v \neq 0} \frac{\ln 2}{4\pi^2 v^2} e^{(2\pi i v / \ln 2) \ln u}.
 \tag{5}$$

The difference between the two is

$$\begin{aligned}
 &\int_1^u \frac{f(v+1)}{v} dv - \int_1^u \frac{f(v)}{v} dv \\
 &= \int_2^{u+1} \frac{f(v)}{v-1} dv - \int_1^u \frac{f(v)}{v} dv \\
 &= \int_2^u \frac{f(v)}{v(v-1)} dv - \int_1^2 \frac{f(v)}{v} dv + \int_u^{u+1} \frac{f(v)}{v-1} dv.
 \end{aligned}$$

An elementary calculation shows that the middle integral is zero and since the function f is uniformly bounded, the last integral vanishes as $u \rightarrow \infty$. The first integral converges absolutely to α defined in Theorem 1. Comparing (2) through (5) with the statement of Theorem 2, we see that its conditions are satisfied with the constants a, b, c , and ρ given by (1) and with Fourier coefficients $c_0 = 0$ and $c_v = -(\ln 2)/(4\pi^2 v^2)$ for $v \neq 0$. This proves Theorem 1.

References

- [1] P.C.P. Bhatt, An interesting way to partition a number, Inform. Process. Lett. 71 (1999) 141–148; <http://www.sciencedirect.com>.
- [2] W.B. Pennington, On Mahler partition problem, Ann. of Math. 57 (1953) 579–589; <http://links.jstor.org>.
- [3] B. Schneier, Applied Cryptography, John Wiley, New York, 1996.