

# Modular Arithmetic Problem in #P

Ohad Asor

January 4, 2016

## Abstract

Given  $n$  integers  $x_1, \dots, x_n$  in binary (or higher) radix, calculating the  $n$  LSB bits of the integer part of  $\prod_{k=1}^n [2^{nx_k} + 2^{-nx_k}]$  is a #P problem. The calculation clearly has a pseudo-polynomial time complexity, as it is polynomial if the input would be supplied in unary format.

Let  $n \in \mathbb{N}, \mathbf{x} \in \mathbb{N}^n$  and consider the formula  $2 \cos a \cos b = \cos(a+b) + \cos(a-b)$  and the cosine being even function to see that:

$$\psi(t) = 2^n \prod_{k=1}^n \cos(x_k t) = \sum_{\sigma \in \{-1,1\}^n} \cos t \langle \mathbf{x}, \sigma \rangle = \sum_{\sigma \in \{-1,1\}^n} e^{it \langle \mathbf{x}, \sigma \rangle} \quad (1)$$

where  $\langle \mathbf{x}, \sigma \rangle = \sum_{k=1}^n \sigma_k x_k$  and counting the number of  $\sigma \in \{-1,1\}^n$  satisfying  $\langle \mathbf{x}, \sigma \rangle = 0$  is a #P problem. We write down the following sum just for fun and substitute (1) in it:

$$S = \frac{1}{n} \sum_{m=1}^n \psi\left(\frac{2\pi m}{n} + i \ln 2\right) = \sum_{\sigma \in \{-1,1\}^n} \frac{2^{-\langle \mathbf{x}, \sigma \rangle}}{n} \sum_{m=1}^n e^{\frac{2\pi i m}{n} \langle \mathbf{x}, \sigma \rangle} \quad (2)$$

multiplying all  $x_k$  by  $n$  (while preserving partitions),  $e^{\frac{2\pi i m}{n} \langle n\mathbf{x}, \sigma \rangle} = 1$  so we get:

$$S = \frac{1}{n} \sum_{m=1}^n \psi\left(\frac{2\pi m}{n} + i \ln 2\right) = \sum_{\sigma \in \{-1,1\}^n} 2^{-n \langle \mathbf{x}, \sigma \rangle} \quad (3)$$

Denoting the number of partitions that sum to  $u$  by

$$c_u = |\{\sigma \in \{-1,1\}^n \mid \langle n\mathbf{x}, \sigma \rangle = u\}| \quad (4)$$

then

$$S = \sum_{u=-\infty}^{\infty} c_u 2^{-u} \quad (5)$$

Recalling that  $\sum_{u=-\infty}^{\infty} c_u = 2^n$  and  $c_u$  are all positive, while in (3) being multiplied by distinct powers  $2^{\pm n}$ , therefore the summands' binary digits never interfere with each other and can never grow as large as 1, except when  $u = 0$ .

Recalling that  $c_0$  is our quantity of interest, we have proved that the number of zero partitions in  $\mathbf{x}$

$$\left\lfloor \frac{2^n}{n} \sum_{m=1}^n \prod_{k=1}^n \cos \left[ nx_k \left( \frac{2\pi m}{n} + i \ln 2 \right) \right] \right\rfloor \mod 2^n \quad (6)$$

$$= \left\lfloor \prod_{k=1}^n [2^{nx_k} + 2^{-nx_k}] \right\rfloor \mod 2^n \quad (7)$$

$$= \left\lfloor 2^{-n \sum_{k=1}^n x_k} \prod_{k=1}^n [1 + 2^{2nx_k}] \right\rfloor \mod 2^n \quad (8)$$

Denote  $s = n \sum_{k=1}^n x_k$  and

$$M = \prod_{k=1}^n [1 + 2^{2nx_k}] = \sum_{\sigma \in \{0,1\}^n} 2^{2n\langle \mathbf{x}, \sigma \rangle} \quad (9)$$

then (8) tells us that the number of zero partitions is encoded as a binary number in the binary digits of  $M$ , from the  $s$ 'th digit to the  $s + n$  digit. We can see right away from (9) that this can be achieved by summing only partitions such that twice their size is between  $s$  and  $s + n$ , or avoiding other partitions.