## Neurophysiological Discoveries of the 2014 Nobel Prize Winners in Medicine from a Computer Arithmetic Perspective



## Behrooz Parhami

Dept. Electrical \& Computer Engr.
Univ. of California, Santa Barbara, USA
parhami@ece.ucsb.edu

Presented at the 20th Int’I Symp. Computer Architecture and Digital Systems Guilan University, Iran, August 2020

## Behrooz Parhami (UCSB), August 2020

## About This Presentation

A preliminary version of this slide show was developed for a talk at Asilomar Conference on Signals, Systems, and Computers, held November 1-4, 2009. Subsequently, the slide show was updated and expanded to incorporate results of new research. All rights reserved for the author. ©2009-2020 Behrooz Parhami

| Edition | Released | Revised | Revised | Revised |
| :--- | :---: | :---: | :---: | :---: |
| First | Nov. 2009 | June 2019 | Aug. 2020 |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Behrogz Parhami (UCSB), August 2020

## Outline

- Introduction / Background
- What were the discoveries?
- Mixed digital/analog arithmetic
- Residue number system (RNS)
- RNS with Continuous Digits (CD-RNS)
- Distinct from conventional RNS
- Motivations for this study
- Dynamic Range and Precision
- Choosing the CD-RNS Moduli
- Conclusions / Future Work



## Behrooz Parhami (UCSB), Ausust 2020

## Abstract

The discovery that mammals use a multi-modular method akin to residue number system (RNS), but with continuous residues or digits, to encode position information led to the award of the 2014 Nobel Prize in Medicine. After a brief review of the evidence in support of this hypothesis, and how it relates to RNS, I discuss the properties of continuous-digit RNS, and present results on the dynamic range, representational accuracy, and factors affecting the choice of the moduli, which are themselves real numbers. I conclude with suggestions for further research on important open problems concerning the process of selection, or evolutionary refinement, of the set of moduli in such a representation.

## Behrooz Parhami (UCSB), Ausust 2020

## Speaker’s Brief Technical Bio

Behrooz Parhami (PhD, UCLA 1973) is Professor of Electrical and Computer Engineering, and former Associate Dean for Academic Personnel, College of Engineering, at University of California, Santa Barbara, where he teaches and does research in the field of computer architecture: more specifically, in computer arithmetic, parallel processing, and dependable computing.


A Life Fellow of IEEE, a Fellow of IET and British Computer Society, and recipient of several other awards (including a most-cited paper award from J. Parallel \& Distributed Computing), he has written six textbooks and more than 300 peer-reviewed technical papers. Professionally, he serves on journal editorial boards (including for 3 different IEEE Transactions) and conference program committees, and he is also active in technical consulting.

## Behrooz Parhami (UCSB), August 2020

## How Looking at Nature Helps my Research

Parallel processing
Parallelism used extensively in human brain and other natural systems


Dependable (fault-tolerant) computing The self-healing amphibian axolotl can regenerate a near-perfect replica of almost any body part it loses


Computer arithmetic
My subject area today: Use of residue representation in rat's navigational system


## Behrogz Parhami (UCSB), August 2020

## Nobel Prize in Physiology or Medicine: 2014

One half went to John O'Keefe (University College, London), the other half to May-Britt Moser (Center for Neural Computation, Norway) and Edvard I. Moser (Kavli Institute for Systems Neuroscience, Norway) "for their discoveries of cells that constitute a positioning system in the brain."


## Behrogz Parhami (UCSB), August 2020

## Sense of Place in Humans and Animals

The sense of place and the ability to navigate are some of the most fundamental brain functions.

German philosopher Immanuel Kant (1724-1804) argued that some mental abilities exist independent of experience.

He considered perception of place as one of these innate abilities through which the external world had to be organized/perceived.


Neurophysiological Discoveries of the 2014 Nobel Prize Winners in Medicine from a Computer Arithmetic Perspective

## Behrogz Parhami (UCSB), August 2020

## The Nobel Laureates' Contributions

John O'Keefe discovered place cells in the hippocampus that signal position and provide the brain with spatial memory capacity.

May-Britt Moser and Edvard I. Moser discovered in the medial entorhinal cortex, a region of the brain next to hippocampus, grid cells that provide the brain with a coordinate system for navigation.

Place cells firings (image from Wikipedia)



Grid cells firings (image from Moser/Rowland/
Moser, 2015)

## First Attempt at Understanding

# What Grid Cells Convey about Rat Location 


#### Abstract

Ila R. Fiete,,$^{1,3}$ Yoram Burak, ${ }^{1,4}$ and Ted Brookings ${ }^{2,5}$ ${ }^{1}$ Kavli Institute for Theoretical Physics and ${ }^{2}$ Department of Physics, University of California, Santa Barbara, Santa Barbara, California 93106, ${ }^{\text {BBroad Fellows }}$ Program, Computation and Neural Systems, California Institute of Technology, Pasadena, California 91125, ${ }^{\text {4 Swartz Fellows Program, Center for Brain }}$ Science, Harvard University, Cambridge, Massachusetts 02138, and ${ }^{5}$ Volen Center, Department of Biology, Brandeis University, Waltham, Massachusetts 02454

We characterize the relationship between the simultaneously recorded quantities of rodent grid cell firing and the position of the rat. The formalization reveals various properties of grid cell activity when considered as a neural code for representing and updating estimates of the rat's location. We show that, although the spatially periodic response of grid cells appears wasteful, the code is fully combinatorial in capacity. The resulting range for unambiguous position representation is vastly greater than the $\approx 1-10 \mathrm{~m}$ periods of individual lattices, allowing for unique high-resolution position specification over the behavioral foraging ranges of rats, with excess capacity that could be used for error correction. Next, we show that the merits of the grid cell code for position representation extend well beyond capacity and include arithmetic properties that facilitate position updating. We conclude by considering the numerous implications, for downstream readouts and experimental tests, of the properties of the grid cell code.


## Behrogz Parhami (UCSB), August 2020

## Localization with Grid Cells

- Rat's navigation system
- Wavy travel path
- Straight return path
- Even in the dark
- Nervous system has place cells \& grid cells - Grid cell firings
- Relative in-cell position
- In-cell positions within several grids pinpoints rat's absolute location

(a) Travel and return paths

(c) Firings and locations [3]

(b) Rat's hexagonal grid

(d) Two hexagonal grids [3]


## Behrogz Parhami (UCSB), August 2020

## The Questions to Be Addressed

- A rat can go up to a certain distance and still be able to find its way back (range)
- Translating grid-cell firings to spatial information
- How the range is related to grid-cell parameters
- Representation range vs. the observed distance
- Fiete, Burak, and Brookings had connected the grid cells to residue representation
- Couldn't confirm the hypothesis theoretically
- Relied on extensive simulation for confirmation


# My First Contribution to the Problem 

© The British Computer Society 2014. All rights reserved. For Permissions, please email: journals.permissions@oup.com

# Digital Arithmetic in Nature: Continuous-Digit RNS 

Behrooz Parhami*<br>University of California, Santa Barbara, CA 93106-9560, USA<br>*Corresponding author: parhami@ece.ucsb.edu


#### Abstract

It has been reported in the literature on computational neuroscience that a rat's uncanny ability to dash back to a home position in the absence of any visual clues (or in total darkness, for that matter) may stem from its distinctive method of position representation. More specifically, it is hypothesized that the rat uses a multimodular method akin to residue number system (RNS), but with continuous residues or digits, to encode position information. After a brief review of the evidence in support of this hypothesis, and how it relates to RNS, we discuss the properties of continuous-digit RNS, and derive results on the dynamic range, representational accuracy and factors affecting the choice of the moduli, which are themselves real numbers. We conclude with suggestions for further research on important open problems concerning the process of selection, or evolutionary refinement, of the set of moduli in such a representation.


## Behrogz Parhami (UCSB), August 2020

## RNS with Analog Digits (Remainders)

- I formulated the spatial representation problem with the grid cells to CD-RNS
- First time RNS is used with analog remainders
- Conventional RNS theory is inapplicable
- I developed a theory for CD-RNS and its range
- Analog and mixed digital-analog technology has a long history in computer arithmetic
- Brief review presented in the next few slides
- More use of analog features expected to come


## Behrogz Parhami (UCSB), August 2020

## Quasi-Digital Parallel Counter

- Analog current summing
- 7 inputs, 3-bit output
- (*): Number of 1 inputs required to produce a 1
- The scheme is even older
- Riordan and Morton, Use of Analog Techniques in Binary Arithmetic Units, IEEE TC, Feb. 1965



## Behrogz Parhami (UCSB), August 2020

## Current-Summing Multivalued Logic

- Binary stored-carry addition
- Limited-carry algorithm
- 3-valued to binary conv.: 3BC


Figures from: Etiemble \& Navi (SMVP, May 1993)

## Behrooz Parhami (UCSB), August 2020

## Mixed D/A Positional Representation

- Continuous-valued number system (CVNS)
- The MSD has all the magnitude info
- Other digits provide successive refinements
- Familiar example: utility meter


Figure from: Saed, Ahmadi, Jullien (IEEE TC, 2002)

## Behrogz Parhami (UCSB), August 2020

## An Ancient Chinese Puzzle

Puzzle, due to the Chinese scholar Sun Tzu, $1500^{+}$years ago:
What number has the remainders of 2,3, and 2 when divided by 7,5 , and 3 , respectively?

Residues (akin to digits in positional systems) uniquely identify the number, hence they constitute a representation: $(2|3| 2)_{\operatorname{RNS}(7|5| 3)}$

In a weird way, RNS is a weighted representation
For RNS(7 | 5 | 3), the weights of the 3 positions are:
$15 \quad 21 \quad 70$

Example -- Chinese puzzle: $(2|3| 2)_{\mathrm{RNS}(7|5| 3)}$ represents the number

$$
\langle 15 \times 2+21 \times 3+70 \times 2\rangle_{105}=\langle 233\rangle_{105}=23
$$

## Behrogz Parhami (UCSB), August 2020

## Residue Number System (RNS)

- Pairwise prime moduli: $m_{k-1}>\ldots>m_{1}>m_{0}$
- Representation of $x:\left\{r_{i}=x \bmod m_{i} \mid 0 \leq i \leq k-1\right\}$
- RNS dynamic range: $M=\prod_{0 \leq i \leq k-1} m_{i}$
- Unsigned in [0, $M$ - 1]
- Signed in [-M/2, M/2 - 1]
- RNS arithmetic algorithms
- Digitwise add, sub, mult
- Difficult div, sign test, compare



## Behrogz Parhami (UCSB), August 2020

## Integer Moduli and Residues

- Two-modulus RNS $\{4,3\}$
- Dynamic range [0, 11]
- Imagine residues with errors
- Errors < 0.5 correctable
- Errors < 1.0 detectable
- Multiresidue systems
- 3-modulus RNS $\{5,4,3\}$
$-\{5,4,3\} \equiv\{20,3\} \equiv\{15,4\} \equiv\{12,5\}$



## Behrogz Parhami (UCSB), August 2020

## Integer Moduli, Continuous Residues

- Residue errors $\varepsilon_{1}$ and $\varepsilon_{0}$
- Decoding error $\leq \max \left(\varepsilon_{1}, \varepsilon_{0}\right)$
- Dynamic range? [0, $12-\varepsilon_{\max }$ ]
- Max allowable error < 0.25



## Behrooz Parhami (UCSB), August 2020

## Continuous Moduli and Residues

Case 1: The moduli are integer multiples of their difference

With proper scaling, the CD-RNS can be converted to an RNS

This example is equivalent to RNS $\{4,3\}$ with scale factor 1.2

## Question:

Are there CD-RNSs that cannot be replaced with ordinary RNSs?


## Behrogz Parhami (UCSB), August 2020

## Equivalence of CD-RNS and RNS

Case 2a: The moduli are integer multiples of some number $s$ (that divides their difference)

With proper scaling, the CD-RNS can be converted to an RNS, provided max error target is $\leq s / 4$ For this example, $s=0.4$ and the system is equivalent to RNS $\{11,9\}$ with scale factor 0.4


## Behrooz Parhami (UCSB), Ausust 2020

## Representational Power of CD-RNS

Case 2b: The moduli are integer multiples of some number $s$ (that divides their difference), but max error target > s/4

The CD-RNS is not equivalent to an RNS in terms of representational capability and dynamic range

For this example, $s=0.1$ but the system is different from RNS $\{65,44\}$ with scale factor 0.1


## Behrogz Parhami (UCSB), August 2020

## Conceptually Simpler 1D Example

- Distance encoded by mod- $a$ and mod- $b$ residues
- Phases $\phi$ and $\psi$ given
- Reverse conversion provides $R$
- $R$ is a point whose mod- $a$ and mod- $b$ residues match $\phi$ and $\psi$ to within the error bound



## Behrogz Parhami (UCSB), August 2020

## Backward Conversion to Binary

- CRT and its derivatives are inapplicable
- Conversion amplifies the errors
- Example 15 in my 2015 Computer Journal paper
- View the conversion as nonlinear optimization
- Convergence occurs with circuit's RC time constant



## Behrogz Parhami (UCSB), August 2020

## Hex Grid Coordinate System

- Point identified by 3 coordinates, one of which is redundant
- Redundancy allows error correction beyond the system's accuracy range



## Behrogz Parhami (UCSB), August 2020

## Open Problems in Neurobiology

- Dynamic range of rat's navigation system
- Numerical simulation: Range $\sim\left(1 / \varepsilon_{\max }\right)^{\text {Exponent }}$ Exponent $\approx$ Number of moduli $-\theta$
- Example: 12 moduli $\Rightarrow$ Exponent $=10.7$

Our results yield an exponent of 11.0

- How did the rat's navigational grids evolve? (Evolutionary basis for moduli optimization)


## Behrogz Parhami (UCSB), August 2020

## Dynamic Range Lower Bound

- CD-RNS with the moduli $\mu_{1}$ and $\mu_{0}$
- $\sigma_{-1}=\mu_{1} ; \sigma_{0}=\mu_{0} ; \sigma_{i+1}=\min \left(\left|\sigma_{i-1}\right|_{\sigma_{i}} \sigma_{i}-\left|\sigma_{i-1}\right|_{\sigma_{i}}\right)$
- Theorem 2: Dynamic range is at least $\left.\left.\mu_{0}\left(1+\left\lfloor\mu_{1} / \mu_{0}\right\rfloor \mu_{0} / \sigma_{1}\right\rfloor\right)\left\lfloor\sigma_{1} / \sigma_{2}\right\rfloor \sigma_{2} / \sigma_{3}\right\rfloor \ldots\left\lfloor\sigma_{j-1} / \sigma_{j}\right\rfloor$ where $j$ is the largest index for which $\sigma_{j} \geq 2 \varepsilon_{\max }$
- Intuition: Remove floors to get $\mu_{0} \mu_{1} /\left(2 \varepsilon_{\text {max }}\right)$
- Example 6: CD-RNS with $\mu_{1}=4.4, \mu_{0}=3.6, \varepsilon_{\max }=0.2$ $\Rightarrow \sigma_{1}=0.8, \sigma_{2}=0.4 \Rightarrow$ Dynamic range $\geq 36.0$


## Behrogz Parhami (UCSB), August 2020

## Dynamic Range Upper Bound

- CD-RNS with the moduli $\mu_{1}$ and $\mu_{0}$
- $\delta$ = Largest number that divides $\mu_{1}$ and $\mu_{0}$ if it exists, 0 otherwise
- Theorem 3: Dynamic range is at most $\left.\max \left(\mu_{0}\left\lfloor\mu_{1} / \gamma\right\rfloor, \mu_{1} L \mu_{0} / \gamma\right\rfloor\right)$ where $\gamma=\max \left(2 \varepsilon_{\max }, \delta\right)$
- Intuition: Remove floors to get $\mu_{0} \mu_{1} / \gamma$
- Example 6: CD-RNS with $\mu_{1}=4.4, \mu_{0}=3.6, \varepsilon_{\max }=0.2$ $\Rightarrow \delta=0.4, \gamma=0.4 \Rightarrow$ Dynamic range $\leq 39.6$


## Behrooz Parhami (UCSB), August 2020

## Lower and Upper Bounds Example

- Example 10 in paper
- Fix $\mu_{1}$ at 4.4
- Vary $\mu_{0}$ in steps of 0.1
- Range varies (dashed)
- Tightness varies
- Matching of upper bound = Optimality?
- Achieving wider range



## Behrogz Parhami (UCSB), August 2020

## Choosing the CD-RNS Moduli

Theorem 2: $\mu \geq 36.0$
Theorem 3: $\mu \leq 39.6$
Intuitively, the moduli are optimal when the two bounds coincide

To cover the dynamic range $\mu$, choose the moduli that are on the order of $\left(2 \mu \varepsilon_{\max }\right)^{1 / 2}$ and differ by $2 \varepsilon_{\max }$


## Behrogz Parhami (UCSB), August 2020

## Conclusions

- Introduced RNS with continuous residues
- Distinct from ordinary RNS
- Advantages (similar to other hybrid schemes)
- Studied range, accuracy, and tradeoffs
- Tight bounds for dynamic range
- Optimal choice of moduli
- Showed link to computational neuroscience
- Rat's sense of location, navigation
- Moduli in nature: evolutionary implications


## Behrooz Parhami (UCSB), August 2020

## Ongoing and Future Work

- Refine and extend the theoretical framework
- Arithmetic and algorithmic implications
- Exact dynamic range, or even tighter bounds
- Study development and application aspects
- Circuit realization and building blocks
- Latency, area, and energy implications
- Pursue links with other hybrid D/A methods
- Mixed implementations?


## Thank You for Your Attention

parhami@ece.ucsb.edu
http://www.ece.ucsb.edu/~parhami/


## Neurophysiological Discoveries of the 2014 Nobel Prize Winners in Medicine from a Computer Arithmetic Perspective



## Behrooz Parhami

Dept. Electrical \& Computer Engr.
Univ. of California, Santa Barbara, USA
parhami@ece.ucsb.edu
Back-up Slides

## Behrogz Parhami (UCSB), August 2020

## RNS Dynamic Range

Product $M$ of the $k$ pairwise relatively prime moduli is the dynamic range

$$
\begin{aligned}
& M=m_{k-1} \times \ldots \times m_{1} \times m_{0} \\
& \text { For } \operatorname{RNS}(8|7| 5 \mid 3), \quad M=8 \times 7 \times 5 \times 3=840
\end{aligned}
$$

Negative numbers: Complement relative to $M$

$$
\begin{array}{rlr}
\langle-x\rangle_{m_{i}} & =\langle M-x\rangle_{m_{i}} & \begin{array}{l}
\text { any otn } \\
\text { consec }
\end{array} \\
21 & =(5|0| 1 \mid 0)_{\mathrm{RNS}} \\
-21 & =(8-5|0| 5-1 \mid 0)_{\mathrm{RNS}}=(3|0| 4 \mid 0)_{\mathrm{RNS}}
\end{array}
$$

Here are some example numbers in our default $\operatorname{RNS}(8|7| 5 \mid 3)$ :

| $(0\|0\| 0 \mid 0)_{\text {RNS }}$ |  |
| :---: | :---: |
|  |  |
| (2\|2|2 |  |
| (0\|1|3 |  |
| (5\|0|1| |  |
| (0\|1| 4 |  |
| (2\|0|0| |  |
| $(7\|6\| 4 \mid 2)_{R}$ |  |

Represents 0 or 840 or . . .
Represents 1 or 841 or ...
Represents 2 or 842 or . . .
Represents 8 or 848 or . . .
Represents 21 or 861 or ...
Represents 64 or 904 or . . .
Represents $\mathbf{- 7 0}$ or 770 or . . .
Represents -1 or 839 or . . .

## Behrogz Parhami (UCSB), August 2020

## RNS Encoding and Arithmetic Operations



Fig. 4.1 Binary-coded format for RNS (8 | 7 | 5 | 3).

Fig. 4.2 The structure of an adder, subtractor, or multiplier for $\operatorname{RNS}(8|7| 5 \mid 3)$.

## Arithmetic in RNS(8|7|5|3)

$$
\text { Represents } x=+5
$$

Operand 1


|  | 5 0 | 2) |
| :---: | :---: | :---: |
|  | 6\| 4 | \| 2$)_{R}$ |
| (4) | 4\|4| | 1 1) |
| (6) | 6\|1| | \| 0) $)_{\text {RN }}$ |
|  |  | $1)_{\text {RN }}$ |

$(5|5| 0 \mid 2)_{\text {RNS }}$
(7|6|4|2) $)_{\text {RNS }}$
$(4|4| 4 \mid 1)_{\mathrm{RNS}}$
(6|6|1|0) 1 RNS
$(3|2| 0 \mid 1)_{\text {RNS }}$

Represents $y=-1$
$x+y:\langle 5+7\rangle_{8}=4,\langle 5+6\rangle_{7}=4$, etc.
$x-y:\langle 5-7\rangle_{8}=6,\langle 5-6\rangle_{7}=6$, etc.
(alternatively, find $-y$ and add to $x$ )
$x \times y:\langle 5 \times 7\rangle_{8}=3,\langle 5 \times 6\rangle_{7}=2$, etc.

## Behrooz Parhami (UCSB), Ausust 2020

## Difficult RNS Arithmetic Operations

Sign test and magnitude comparison are difficult
Example: Of the following $\operatorname{RNS}(8|7| 5 \mid 3)$ numbers:
Which, if any, are negative?
Which is the largest?
Which is the smallest?
Assume a range of [-420, 419]

$$
\begin{array}{lll}
a=(0|1| 3 \mid 2)_{\text {RNS }} & \\
b=(0|1| 4 \mid 1)_{\text {RNS }} & \text { Answers: } \\
c=(0|6| 2 \mid 1)_{\text {RNS }} & d<c<f<a<e<b \\
d=(2|0| 0 \mid 2)_{\text {RNS }} & -70<-8<-1<8<21<64 \\
e=(5|0| 1 \mid 0)_{\text {RNS }} & \\
f=(7|6| 4 \mid 2)_{\text {RNS }} &
\end{array}
$$

## Behrogz Parhami (UCSB), August 2020

## Forward and Reverse Conversions



The more the amount of computation performed between the initial forward conversion and final reverse conversion (reconversion), the greater the benefits of RNS representation.

## Behrooz Parhami (UCSB), Ausust 2020

## Intuitive Justification for CRT

Puzzle: What number has the remainders of 2,3 , and 2 when divided by the numbers 7,5 , and 3 , respectively?

$$
x=(2|3| 2)_{\mathrm{RNS}(7| | \mid 3)}=(?)_{\mathrm{ten}}
$$

$(1|0| 0)_{\text {RNS }(7|5| 3)}=$ multiple of 15 that is $1 \bmod 7=15$
$(0|1| 0)_{\text {RNS }(7| | \mid 3)}=$ multiple of 21 that is $1 \bmod 5=21$
$(0|0| 1)_{\mathrm{RNS}(7| | \mid 3)}=$ multiple of 35 that is $1 \bmod 3=70$
$(2|3| 2)_{R N S(7| | \mid 3)}=(2|0| 0)+(0|3| 0)+(0|0| 2)$ $=2 \times(1|0| 0)+3 \times(0|1| 0)+2 \times(0|0| 1)$
$=2 \times 15+3 \times 21+2 \times 70$
$=30+63+140$
$=233=23 \bmod 105$
Therefore, $x=(23)_{\text {ten }}$

## Behrooz Parhami (UCSB), Ausust 2020

## Example RNS with Special Moduli

For $\operatorname{RNS}(17|16| 15)$, the weights of the 3 positions are:

$$
\begin{array}{lll}
2160 & 3825 & 2176
\end{array}
$$

Example: $\left(x_{2}, x_{1}, x_{0}\right)=(2|3| 4)_{\text {RNS }}$ represents the number

$$
\langle 2160 \times 2+3825 \times 3+2176 \times 4\rangle_{4080}=\langle 24,499\rangle_{4080}=19
$$

$2160=2^{4} \times\left(2^{4}-1\right) \times\left(2^{3}+1\right)=2^{11}+2^{7}-2^{4}$
$3825=\left(2^{8}-1\right) \times\left(2^{4}-1\right)=2^{12}-2^{8}-2^{4}+1$
$2176=2^{7} \times\left(2^{4}+1\right)=2^{11}+2^{7}$
$4080=2^{12}-2^{4}$; thus, to subtract 4080, ignore bit 12 and add $2^{4}$
Reverse converter: Multioperand adder, with shifted $x_{i} s$ as inputs

## Behrooz Parhami (UCSB), Ausust 2020

## Limits of Fast Arithmetic in RNS

## Known results from number theory

Theorem 4.2: The $i$ th prime $p_{i}$ is asymptotically $i \ln i$
Theorem 4.3: The number of primes in $[1, n]$ is asymptotically $n / \ln n$
Theorem 4.4: The product of all primes in $[1, n]$ is asymptotically $e^{n}$
Implications to speed of arithmetic in RNS
Theorem 4.5: It is possible to represent all $k$-bit binary numbers in RNS with $\mathrm{O}(k / \log k)$ moduli such that the largest modulus has $\mathrm{O}(\log k)$ bits

That is, with fast log-time adders, addition needs $\mathrm{O}(\log \log k)$ time

