Number Systems and Cryptography

Jean Claude Bajard

Sorbonne Université

JMM 2025 Lyon

Motivations

- **At the origine: Redundant number systems, on-line computing...**
  - J. Duprat and J.M. Muller, Ecrire les nombres autrement pour calculer plus vite, Technique et Science Informatique, Vol. 10 No 3, 1991.
  - Y. Herreros. Contribution à l'arithmétique des ordinateurs. Modélisation et simulation. Institut National Polytechnique de Grenoble - INPG, 1991.
  - On-line arithmetic: An overview MD Ercegovac - Real-Time Signal Processing VII, 1984
- **A milestone:** D. Gamberger, "New approach to integer division in residue number systems," 10th IEEE Symposium on Computer Arithmetic, Grenoble, France, 1991
- **Then cryptography:** use of huge numbers or polynomials, modular operations, exponentiations etc...

Number Systems and Cryptography

Residue Systems

Residue Systems

Residue Number Systems

(CRT) Ch'in Chiu-Shao 1247, Svoboda-Valach'57, Garner'59, Szabo-Tanaka'67

RNS Base

- A set of coprime numbers $\mathcal{B} = (m_1, ..., m_k)$ with $M = \prod_{i=1}^{k} m_i$

Representation in RNS (Chinese Remainder Theorem)

- $0 \leq A < M$ represented by its residues $(a_1, ..., a_k)$ with $a_i = A \bmod m_i = |A|_{m_i}$

Operations

- Full parallel operations $\pmod M$
  $(|a_1 \circ b_1|_{m_1}, \ldots, |a_n \circ b_n|_{m_n}) \rightarrow A \circ B \pmod M$
  ($\circ$ for addition, multiplication or exact division by an invertible number)

Residue Systems





RNS version of Montgomery Reduction

(Posh-Posh 1995), (B.-Didier-Kornerup 1997 2001), (Kawamura-Koike-Sano-Shimbo 2000)

RNS Montgomery algorithm: Montg$(A, \mathcal{B}, \mathcal{B}', P)$

1. $Q_{\mathcal{B}} = A_{\mathcal{B}}(-P^{-1})_{\mathcal{B}}$ (modulo M in base $\mathcal{B} = (m_1, ..., m_k)$)
2. Extension of the representation of $Q_{\mathcal{B}}$ to the base $\mathcal{B}' = (m'_1, ..., m'_k)$
3. $R_{\mathcal{B}'} = (A_{\mathcal{B}'} + Q_{\mathcal{B}'} P_{\mathcal{B}'}) \times M^{-1}_{\mathcal{B}'}$ (modulo M' in base $\mathcal{B}'$)
4. Extension of the representation of R to the base $\mathcal{B}$

Remarks

M' and M coprime (existence of M^{-1} mod M')

$R \equiv A \times M^{-1}$ mod P with $R < 2P$ if $A < MP$ and $2P < M, M'$

And A mod $P =$ Montg$(R \times (M^2 \bmod P), \mathcal{B}, \mathcal{B}', P)$

RNS version of Montgomery Reduction

(Posh-Posh 1995), (B.-Didier-Kornerup 1997 2001), (Kawamura-Koike-Sano-Shimbo 2000)

RNS Montgomery algorithm: $\mathrm{Montg}(A, \mathcal{B}, \mathcal{B}', P)$

1. $Q_{\mathcal{B}} = A_{\mathcal{B}}(-P^{-1})_{\mathcal{B}}$ (modulo M in base $\mathcal{B} = (m_1, ..., m_k)$)
2. Extension of the representation of $Q_{\mathcal{B}}$ to the base $\mathcal{B}' = (m'_1, ..., m'_k)$
3. $R_{\mathcal{B}'} = (A_{\mathcal{B}'} + Q_{\mathcal{B}'} P_{\mathcal{B}'}) \times M^{-1}_{\mathcal{B}'}$ (modulo M' in base $\mathcal{B}'$)
4. Extension of the representation of R to the base $\mathcal{B}$

Remarks

M' and M coprime (existence of $M^{-1} \bmod M'$)

$R \equiv A \times M^{-1} \bmod P$ with $R < 2P$ if $A < MP$ and $2P < M, M'$

And $A \bmod P = \mathrm{Montg}(R \times (M^2 \bmod P), \mathcal{B}, \mathcal{B}', P)$

Montgomery notation

$A' = A \times M \bmod P$ and $\mathrm{Montg}(A' \times B', \mathcal{B}, \mathcal{B}', P) \equiv (A \times B) \times M \pmod P$

$A' = \mathrm{Montg}(A \times (M^2 \bmod P), M, M', P)$

Some conclusions about RNS

(B. - Duquesne - Ercegovac - Meloni 2006), (Szerwinski - Güneysu 2008), (Guillermin 2010), (Antão - B. - Sousa 2010), (Duquesne 2011) (B, J Eynard, M. A Hasan, V Zucca 2016_{SAC}), (SEAL Microsoft 2018), (Halevi-Polyakov-Shoup $2019_{CT-RSA\cdot}$) (B. - Duquesne 2021) (M. Vollmer - K. Bigou - A.Tisserand 2025)

- RNS is well adapted to parallel architectures (GPU, Multicore,...), and FPGA or ASIC.
- Modular reductions stay costly. As for the interpolation, the choice of the bases is important.
- For some cryptographic computations huge integers. With ECC or Pairing it is possible to reduce the number of modular reductions.
- Randomized arithmetics, leak resistant arithmetics.
- Approximate RNS rounding: CVP (Babai), Homomorphic Encryption (RLWE,FV,BGV) (**??**)
- Montgomery friendly numbers

Modular Positional Arithmetics





Modular Positional Arithmetics





Example $(a + b \times 10)$ modulo 13

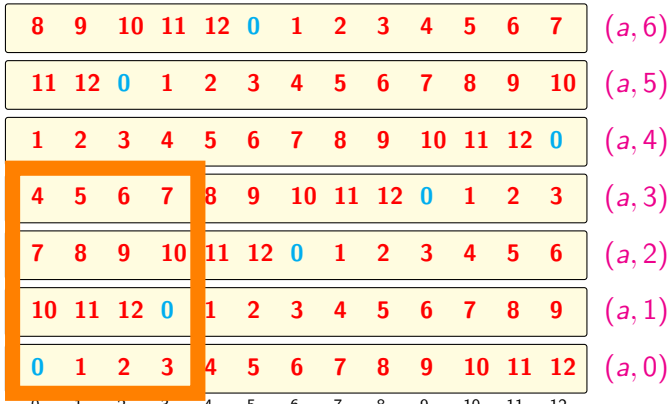
8	9	10	11	12	0	1	2	3	4	5	6	7	$(a, 6)$
11	12	0	1	2	3	4	5	6	7	8	9	10	$(a, 5)$
1	2	3	4	5	6	7	8	9	10	11	12	0	$(a, 4)$
4	5	6	7	8	9	10	11	12	0	1	2	3	$(a, 3)$
7	8	9	10	11	12	0	1	2	3	4	5	6	$(a, 2)$
10	11	12	0	1	2	3	4	5	6	7	8	9	$(a, 1)$
0	1	2	3	4	5	6	7	8	9	10	11	12	$(a, 0)$
0	1	2	3	4	5	6	7	8	9	10	11	12	

Example $(a + b \times 10)$ modulo 13

8	9	10	11	12	0	1	2	3	4	5	6	7	$(a, 6)$
11	12	0	1	2	3	4	5	6	7	8	9	10	$(a, 5)$
1	2	3	4	5	6	7	8	9	10	11	12	0	$(a, 4)$
4	5	6	7	8	9	10	11	12	0	1	2	3	$(a, 3)$
7	8	9	10	11	12	0	1	2	3	4	5	6	$(a, 2)$
10	11	12	0	1	2	3	4	5	6	7	8	9	$(a, 1)$
0	1	2	3	4	5	6	7	8	9	10	11	12	$(a, 0)$
0	1	2	3	4	5	6	7	8	9	10	11	12	

with digits $\{0, 1, 2, 3, 4\}$

Example $(a + b \times 10)$ modulo 13



with digits $\{0, 1, 2, 3\}$

Example $(a + b \times 10)$ modulo 13

8	9	10	11	12	0	1	2	3	4	5	6	7	$(a, 6)$
11	12	0	1	2	3	4	5	6	7	8	9	10	$(a, 5)$
1	2	3	4	5	6	7	8	9	10	11	12	0	$(a, 4)$
4	5	6	7	8	9	10	11	12	0	1	2	3	$(a, 3)$
7	8	9	10	11	12	0	1	2	3	4	5	6	$(a, 2)$
10	11	12	0	1	2	3	4	5	6	7	8	9	$(a, 1)$
0	1	2	3	4	5	6	7	8	9	10	11	12	$(a, 0)$
0	1	2	3	4	5	6	7	8	9	10	11	12	

with digits $\{0, 1, 2, 3\}$

$$(1, 1) \times (2, 1) = (1 + x) \times (2 + x) = 2 + 3x + x^2 = (2, 3, 1)$$

Example $(a + b \times 10)$ modulo 13

8	9	10	11	12	0	1	2	3	4	5	6	7	$(a, 6)$
11	12	0	1	2	3	4	5	6	7	8	9	10	$(a, 5)$
1	2	3	4	5	6	7	8	9	10	11	12	0	$(a, 4)$
4	5	6	7	8	9	10	11	12	0	1	2	3	$(a, 3)$
7	8	9	10	11	12	0	1	2	3	4	5	6	$(a, 2)$
10	11	12	0	1	2	3	4	5	6	7	8	9	$(a, 1)$
0	1	2	3	4	5	6	7	8	9	10	11	12	$(a, 0)$
0	1	2	3	4	5	6	7	8	9	10	11	12	

with digits $\{0, 1, 2, 3\}$

$$(1, 1) \times (2, 1) = (1 + x) \times (2 + x) = 2 + 3x + x^2 = (2, 3, 1)$$

$100 \bmod 13 = 9 = (2, 2)$ so $(1, 1) \times (2, 1) = (2, 3) + (2, 2) = (4, 5) \Rightarrow (2, 0)$

Example $(a + b \times 10)$ modulo 13

with digits $\{0, 1, 2, 3\}$

$$(1,1) \times (2,1) = (1+x) \times (2+x) = 2 + 3x + x^2 = (2,3,1)$$

$100 \bmod 13 = 9 = (2,2)$ so $(1,1) \times (2,1) = (2,3) + (2,2) = (4,5) \Rightarrow (2,0)$

Example $(a + b \times 10)$ modulo 13

with digits $\{0, 1, 2, 3\}$

$$(1, 1) \times (2, 1) = (1 + x) \times (2 + x) = 2 + 3x + x^2 = (2, 3, 1)$$

$100 \bmod 13 = 9 = (2, 2)$ so $(1, 1) \times (2, 1) = (2, 3) + (2, 2) = (4, 5) \Rightarrow (2, 0)$

Example $(a + b \times 10)$ modulo 13

8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
11	12	0	1	2	3	4	5	6	7	8	9	10	11	12	0	1
1	2	3	4	5	6	7	8	9	10	11	12	0	1	2	3	4
4	5	6	7	8	9	10	11	12	0	1	2	3	4	5	6	7
7	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10
10	11	12	0	1	2	3	4	5	6	7	8	9	10	11	12	0
0	1	2	3	4	5	6	7	8	9	10	11	12	0	1	2	3
-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13

$(a, 5)$

$(a, 4)$

$(a, 3)$

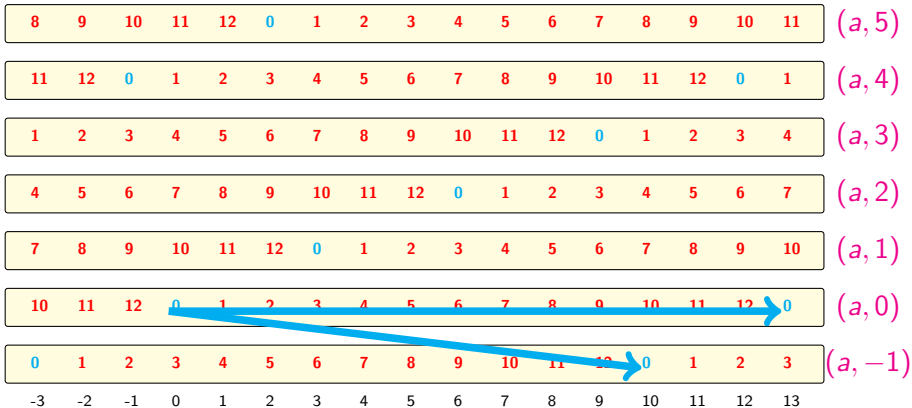
$(a, 2)$

$(a, 1)$

$(a, 0)$

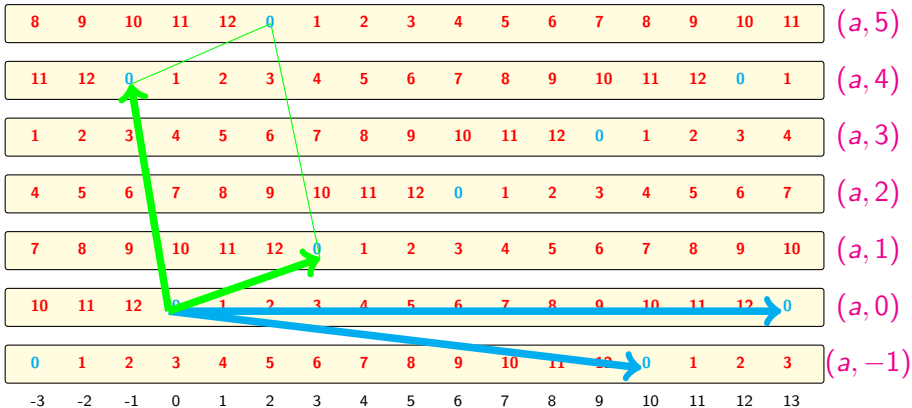
$(a, -1)$

Example $(a + b \times 10)$ modulo 13



base of the lattice $\begin{pmatrix} 10 & -1 \\ 13 & 0 \end{pmatrix}$

Example $(a + b \times 10)$ modulo 13



base of the lattice $\begin{pmatrix} 10 & -1 \\ 13 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & 4 \\ 3 & 1 \end{pmatrix}$

Polynomial Modular Number Systems

Th. Plantard 2005$_{Phd}$

Definition of the PMNS

- Representation of $A \in \mathbb{F}_p$:

  $A = \sum_{i=0}^{n-1} a_i \gamma^i \bmod p$, with $a_i \in \{0, ..., \rho - 1\}$ and $p < \rho^n$

- γ can be huge, but ρ is small (redundancy)
- $E(X) = X^n - \varepsilon(X)$ such that $E(\gamma) \equiv 0 \pmod p$ with ε "small" polynomial
- (p, n, γ, ρ, E) is a PMNS if all elements of $\mathbb{F}_p$ can be represented

Polynomial Modular Number Systems

Th. Plantard 2005$_{Phd}$

Definition of the PMNS

- Representation of $A \in \mathbb{F}_p$:

  $A = \sum_{i=0}^{n-1} a_i \gamma^i \bmod p$, with $a_i \in \{0, ..., \rho - 1\}$ and $p < \rho^n$

- γ can be huge, but ρ is small (redundancy)
- $E(X) = X^n - \varepsilon(X)$ such that $E(\gamma) \equiv 0 \pmod p$ with ε "small" polynomial
- (p, n, γ, ρ, E) is a PMNS if all elements of $\mathbb{F}_p$ can be represented

Modular Multiplication: $A \times B \bmod p$

- $C(X) = A(X) \times B(X) \bmod E(X)$ with $A(\gamma) \bmod p = A$ and $B(\gamma) \bmod p = B$
- Reduction of the coefficients of $C(X)$ (Babai, Montgomery...)
- $C(\gamma) \equiv A \times B \pmod p$

Polynomial Modular Number Systems

B. - Imbert - Plantard [2005], B.-Marrez-Plantard-Veron [2020]

Find ρ and γ for a given P

Consider the modulo $p = 53$, and $n = 7$ for the digit size, $p < \rho^7$, and we expect a small value for ρ like $\rho = 2$.

We look for a radix with Pseudo-Mersenne property, (generally an irreducible polynomial)

We find $\gamma = 14$, such that $\gamma^7 \equiv 2 \pmod{p}$ and $E(X) = X^7 - 2$.

We consider the carry propagation lattice modulo p

$$L = \begin{pmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \\ V_6 \\ V_7 \end{pmatrix} = \begin{pmatrix} -14 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -14 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -14 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -14 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -14 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -14 & 1 \\ 53 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Polynomial Modular Number Systems

B. - Imbert - Plantard 2005, B.-Marrez-Plantard-Veron2020

Remarks and construction

- This lattice L admits as short vector

$(1, 1, 0, 0, 0, 0, 1) = V_6 + 14 * V_5 + 14^2 * V_4 + 14^3 * V_3 + 14^4 * V_2 + (14^5 + 1) * V_1 + V_7$

- With $\gamma^7 \equiv 2 \pmod{p}$, we construct a sublattice L'.

$$\Rightarrow L' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 2 & 1 \end{pmatrix}$$

- Hence, we can take $\rho \geq 5$ (for digits in $\{0, ..., 4\}$ or $\{-2, ..., 2\}$)
- Coefficient reduction becomes a closest vector problem

Number of PMNS for a given p

B. - Imbert - Plantard $_{2005}$,B.-Marrez-Plantard-Veron$_{2020}$

We consider $p = 782647469246946003938740009999297$ (113 bits) and $E(X) = X^5 + X^2 + 1$.

$\gcd(X^p - X, E(X)) \bmod p$

$= \gcd(X^p \bmod E(X) - X, E(X)) \bmod p$

$= X^2 + 130584999841906729100033789770525 8\, X + 17930730009542045460341940680988 26$

$= (X + 615769903955780927067106889507091 2)(X + 297462565133071805971666910263364 3)$

Hence, we obtain two roots of $E(X) \bmod p$:

$\gamma_1 = 166877565291165076871633120492838 5$

$\gamma_2 = 485184904113874197967073099736565 4$

For γ_1 and γ_2 we can have $\rho < 2^{23}$ (for digits in $\{-\rho, ..., \rho\}$) which is close to be optimal.

Conclusions

- The polynomial reduction (after a product for example) is very efficient
- The coefficient reduction was efficient in a first approach where a power of 2 must have a particular small representation in PMNS. In this case p is constructed
- The Montgomery coefficient reduction has a cost but recent papers improved it
- The coefficient reduction remains the big challenge

Modular Positional Arithmetics





Ostrowski Bases (1921)

(modular multiplication $a \times b \bmod m$)

Continued Fraction Expansion of $\frac{a}{m}$ $\gcd(a, m) = 1$ and convergents

- $\frac{a}{m} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \dots}}}$ et $\frac{p_i}{q_i} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cdots \cfrac{1}{k_i}}}$
- $\theta_i = aq_i - mp_i$

Ostrowski Bases (1921)

(modular multiplication $a \times b \bmod m$)

Continued Fraction Expansion of $\frac{a}{m}$ $\gcd(a, m) = 1$ and convergents

- $\frac{a}{m} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \dots}}}$ et $\frac{p_i}{q_i} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cdots \frac{1}{k_i}}}$
- $\theta_i = aq_i - mp_i$
- Recursive computation

$$
\begin{array}{llll}
T_{i+1} & = \frac{1}{T_i - k_i} & T_0 = \frac{a}{m} & k_i = \lfloor T_i \rfloor \\
q_{i+2} & = k_{i+2} q_{i+1} + q_i & q_0 = 1 & q_{-1} = 0 \\
\theta_{i+2} & = k_{i+2} \theta_{i+1} + \theta_i & \theta_0 = a - m k_0 & \theta_{-1} = -m
\end{array}
$$

Ostrowski Bases (1921)

(modular multiplication $a \times b \bmod m$)

Continued Fraction Expansion of $\frac{a}{m}$ $\gcd(a, m) = 1$ and convergents

- $\frac{a}{m} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \dots}}}$ et $\frac{p_i}{q_i} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cdots \frac{1}{k_i}}}$
- $\theta_i = aq_i - mp_i$
- Recursive computation

$$\begin{array}{lll} T_{i+1} = \frac{1}{T_i - k_i} & T_0 = \frac{a}{m} & k_i = \lfloor T_i \rfloor \\ q_{i+2} = k_{i+2} q_{i+1} + q_i & q_0 = 1 & q_{-1} = 0 \\ \theta_{i+2} = k_{i+2} \theta_{i+1} + \theta_i & \theta_0 = a - mk_0 & \theta_{-1} = -m \end{array}$$

Ostrowski representations base (q_i) and base (θ_i)

$$b = \sum_{i=0}^{n-1} b_i q_i, \quad \text{with } b_0 < k_1,\ 0 \le b_i \le k_{i+1},\ b_i = 0 \text{ if } b_{i+1} = k_{i+2}$$

$$x = \sum_{i=0}^{n-1} x_i \theta_i, \quad \text{with } x_0 < k_1,\ 0 \le x_i \le k_{i+1},\ x_i = 0 \text{ if } x_{i+1} = k_{i+2}$$

Ostrowski Bases

Example

Continued Fraction Expansion of $\frac{3238}{7741}$

- $\frac{3238}{7741} = [0; 2, 2, 1, 1, 3, 1, 2, 4, 1, 2, 3]$
- Ostrowski base (q)

$$B_q := [1, 2, 5, 7, 12, 43, 55, 153, 667, 820, 2307]$$

- Consider $b = 6000$ in Ostrowski representation

$$b_{B_q} := [0, 1, 0, 1, 0, 1, 1, 3, 0, 1, 2]$$

- $x := [1, 0, 1, 0, 3, 0, 2, 0, 1, 0, 3]$ represents 7740 the largest value

Ostrowski Bases

Example

Continued Fraction Expansion of $\frac{3238}{7741}$

- θ base

$$B_\theta := [3238, -1265, 708, -557, 151, -104, 47, -10, 7, -3, 1]$$

- Decreases and Alternates
- $x := [1, 0, 1, 0, 3, 0, 2, 0, 1, 0, 3]$ represents 4503 the largest value
- $y := [0, 2, 0, 1, 0, 1, 0, 4, 0, 2, 0]$ represents -3237 the smallest value
- Remark: $x - y = 7740$

Ostrowski Bases and Multiplication

M. Gouicem 2013$_{PhD}$

Computation of $a \times b \mod m$

1. Evaluation of q_i and θ_i from $\frac{a}{m}$.

Ostrowski Bases and Multiplication

M. Gouicem 2013$_{PhD}$

Computation of $a \times b \mod m$

1. Evaluation of q_i and θ_i from $\frac{a}{m}$.
2. Representation of b in the Ostrowski base (q_i).

$$b = \sum_{i=0}^{n-1} b_i q_i, \quad \text{with } b_0 < k_1,\ 0 \leq b_i \leq k_{i+1},\ b_i = 0 \text{ if } b_{i+1} = k_{i+2}$$

Ostrowski Bases and Multiplication

M. Gouicem 2013$_{PhD}$

Computation of $a \times b \mod m$

1. Evaluation of q_i and θ_i from $\frac{a}{m}$.
2. Representation of b in the Ostrowski base (q_i).

$$b = \sum_{i=0}^{n-1} b_i q_i, \quad \text{with } b_0 < k_1,\ 0 \leq b_i \leq k_{i+1},\ b_i = 0 \text{ if } b_{i+1} = k_{i+2}$$

3. Return $R = \sum_{i=0}^{n-1} b_i \theta_i = a \cdot b \mod m$, with $(-m < R < m)$

Proof: $\sum_{i=0}^{n-1} b_i \theta_i = \sum_{i=0}^{n-1} b_i (a q_i - m p_i) = a \sum_{i=0}^{n-1} b_i q_i + \alpha m$

Ostrowski Bases

Example

Multiplication of $3238 \times 6000 \pmod{7737}$

- $\frac{3238}{7741} = (0, 2, 2, 1, 1, 3, 1, 2, 4, 1, 2, 3)$

  $B_q := [1, 2, 5, 7, 12, 43, 55, 153, 667, 820, 2307]$

  $B_\theta := [3238, -1265, 708, -557, 151, -104, 47, -10, 7, -3, 1]$

- Consider $b = 6000$ in Ostrowski representation $b_{B_q} := [0, 1, 0, 1, 0, 1, 1, 3, 0, 1, 2]$
- We obtain in θ base

  $(1 * (-1265) + 1 * (-557) + 1 * (-104) + 1 * 47 + 3 * (-10) + 1 * (-3) + 2 * 1)$

  $= (-1910) \equiv 5831 \equiv 3238 \times 6000 \bmod 7741$

Conclusions

- Quadratic complexity in the size of the modulo.
- Division: the θ representation provides the division in Ostrowski representation.
- Allow to perform inversion, multiplication and division with the same circuit.
- Multiplications and/or divisions by the same number a becomes efficient

Exponent representations

Exponent representations

Addition Chains: Fibonacci - Zeckendorf

Representation of Zeckendorf - 1972 (1939)

- Fibonacci Series: $F_{n+2} = F_{n+1} + F_n$, with $F_0 = 0$ and $F_1 = 1$
  $1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$
- Representation with $q_i = F_{i+2}$

$$b = \sum_{i=1}^{n-1} b_i q_i, \quad \text{with } b_i \in \{0,1\},\ b_i = 0 \text{ if } b_{i+1} = 1$$

Remarks

- It is the Ostrowski representation using the continued fraction expansion of the golden ratio.
- Example: $k := 1117 = [0,1,0,1,0,0,0,1,0,1,0,0,0,0,1]_{\mathcal{Z}} = F_3 + F_5 + F_9 + F_{11} + F_{16} = 2 + 5 + 34 + 89 + 987$

Addition Chains: Fibonacci - Zeckendorf

kP with an efficient $P + Q$.

- Algorithm:
  1. Decomposition in the Fibonacci representation
  2. Recursive computing with respect to the decomposition
- Example: Evaluation right to left of $1117.P$ using $[0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1]_{\mathcal{Z}}$ with 18 Additions

1	0	0	0	0	1	0	1	0	0	0	1	0	1	0
1	1	2	3	5	8									
					9	14	23							
							24	38	62	100	162			
											163	263	426	
													427	690	1117

Addition Chains: Fibonacci - Zeckendorf

E. B. Burger et al. 2012$_{ActaAr.}$

Properties

- Length: k such that $F_k \leq n < F_{k+1}$
- Ratio of ones: $\frac{\psi(k)}{k} \to \frac{5-\sqrt{5}}{10} = 0.2763$

Pros and cons

- Advantage: only additions
- Drawback: more digits than in binary: ratio $= \frac{\ln 2}{\ln \varphi} \sim 1.44$ with $\varphi = \frac{1+\sqrt{(5)}}{2}$
- Tool: Greedy Algorithm

Euclidean Addition Chains

N. Meloni 2007$_{PhD}$, Herbaut-Liardet-Meloni-Teglia-Veron 2010$_{INDOCRYPT}$, Dosso - Herbaut - Meloni - Véron 2018$_{JCE}$, Bos - Friedberger 2018$_{IEEETC}$

Definition

A Euclidean addition chain (EAC) of length s for an integer k is a sequence $(c_i)_{i=1...s}$ with $c_i \in \{0, 1\}$.

The computation of k is obtained from the sequence $(v_i, u_i)_{i=0..s}$

$v_0 = 1,\ u_0 = 1$

$(u_i, v_i) = (v_{i-1} + u_{i-1}, v_{i-1})$ if $c_i = 1$ (small step),

$(u_i, v_i) = (v_{i-1} + u_{i-1}, u_{i-1})$ if $c_i = 0$ (big step).

Then we denote $\chi(c) = v_s + u_s = k$.

Properties

- Euclidean algorithm scheme
- $\chi(0_n) = F_{n+3}$, $\chi(1_n) = n + 2$

Euclidean Addition Chains

N. Meloni 2007$_{PhD}$, Herbaut-Liardet-Meloni-Teglia-Veron 2010$_{INDOCRYPT}$, Dosso - Herbaut - Meloni - Véron 2018$_{JCE}$, Bos - Friedberger 2018$_{IEEETC}$

Example

We can find shorter chains for 1117 with 15 additions:

$$1117 \leftarrow [648, 469], [469, 179],$$
$$[290, 179], [179, 111], [111, 68], [68, 43], [43, 25], [25, 18], [18, 7],$$
$$[11, 7], [7, 4], [4, 3], [3, 1],$$
$$[2, 1], [1, 1]$$

$$\chi(01000100000010) = 1117$$

Construction of keys

How to construct a set of keys with efficient EAC representations?

Exponent representations

Double base

Dimitrov-Jullien-Miller 1999$_{ieeeTC}$, Dimitrov-Imbert-Mishra 2005$_{ASIACRYPT}$

Double Base

- Representation: $X = \sum x_{i,j} 2^i 3^j, \quad x_{i,j} \in \{0,1\}$
- Example: $127 = 1111111_b = 2^3 3^2 + 2^1 3^3 + 2^0 3^0 = 72 + 54 + 1$

kP with $2P$ and $3P$

1. Decomposition in double base, find a path.
2. Return $2^{i_0} 3^{j_0} P + 2^{i_1} 3^{j_1} P + 2^{i_2} 3^{j_2} P + \ldots$

Advantages and Drawbacks

- Sparse representation
- Redundancy and optimal representation




Double base

Berthé - Imbert 2009$_{DMTCS}$, Tijdeman 1974$_{CompMath}$

Construction

- How to find the nearest $2^a 3^b$ to a given number N?
- Then a greedy algorithm can be used.
- Number of non-zero digits is in $O(\log N / \log\log N)$

Method

- We minimize: $a * \ln 2 + b * \ln 3 - \ln N$ or $a \log_3 2 + b - \log_3 N$
- Considering the fractional part we have $(a \log_3 2 - \log_3 N) \bmod 1$

Double base

Berthé - Imbert 2009$_{DMTCS}$

Method using Ostrowski

- We consider the continued fraction expansion of $\log_3 2$
  $[0; 1, 1, 1, 2, 2, 3, 1, 5, 2, 23, 2, ...]$
- The Ostrowski bases are constructed
  - $\theta_i = q_i * \log_3 2 - p_i$
  - Recursive computation $\begin{array}{llll} q_{i+2} & = k_{i+2}q_{i+1} + q_i & q_0 = 1 & q_{-1} = 0 \\ \theta_{i+2} & = k_{i+2}\theta_{i+1} + \theta_i & \theta_0 = \log_3 2 - k_0 & \theta_{-1} = -1 \end{array}$
- a is found in two steps
  - Representation of $\log_3 N$ mod 1 in θ base: $(\log_3 N) \bmod 1 = \sum_{i=0}^{n-1} n_i\theta_i$
  - We have $a = \sum_{i=0}^{n-1} n_i q_i$

Double base

Berthé - Imbert 2009$_{DMTCS}$

Example for $N = 2000$

- We consider the continued fraction expansion of $\log_3 2$: $[0; 1, 1, 1, 2, 2]$
  and the bases: $B_q = [1, 1, 2, 3, 8, 19]$ $B_\theta = [0.63, -0.369, 0.26, -.1, 0.047, -0.012]$
- we consider $T = (\log_3 N - \lfloor \log_3 N \rfloor) = 0.918639575$
  - $T_\theta = [1, 0, 1, 0, 0, 0] = 0.8927892604$
  - In the base B_q: $[1, 0, 1, 0, 0, 0] = 3 = a$
  - Then $\lfloor \log_3(N/2^3) \rfloor = 5 = b$
- We verify that:

$2^1 3^6$	$2^3 3^5$	$2^4 3^4$	$2^6 3^3$	$2^7 3^2$	$2^9 3^1$	$2^{10} 3^0$
1458	1944	1296	1728	1152	1536	1024

Conclusions





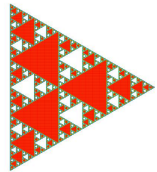
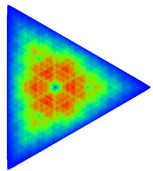
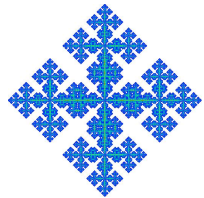
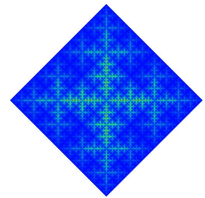
Conclusions

Some are quite popular

- Residue Number Systems
- Addition Chains
- Double bases

Some not yet

- PMNS
- Ostrowski

Thank you!