Study Of Different Arithmatic Operations Number System Polynomial

Baljit Singh

Research Scholar, Manav Bharti University, H.P., India

ABSTRACT: We propose a new number representation and arithmetic for the elements of the ring of integers modulo p. The so- called Polynomial Modular Number System (PMNS) allows for fast polynomial arithmetic and easy parallelization. The most important contribution of this paper is the fundamental theorem of a Modular Number System, which provides a bound for the coefficients of the polynomials used to represent the set $\mathbb{Z}_p$. However, we also propose a complete set of algorithms to perform the arithmetic operations over a PMNS, which make this system of practical interest for people concerned about efficient implementation of modular arithmetic.

----------♦----------

1. INTRODUCTION

Efficient implementation of modular arithmetic is an important prerequisite in today's public-key cryptography [10]. The celebrated RSA algorithm [13], and the cryptosystems based on the discrete logarithm problem, such as Diffie-Hellman key exchange [6], need fast arithmetic modulo integers of size 1024 to roughly 15000 bits. For the same level of security, elliptic curves defined over prime fields, require operations modulo prime numbers whose size range approximately from 160 to 500 bits [8].

Classic implementations use multiprecision arithmetic, where long integers are represented in a predefined high-radix (usually a power of two depending on the word size of the targeted architecture). Arithmetic operations, namely modular reduction and multiplication, are performed using efficient algorithms, such as as Montgomery [12], or Barrett [3]. (For more details, see [10], chapter 14.) These general algorithms do not require the divisor, also called modulus, to be of special form. When this is the case, however, modular multiplication and reduction can be accelerated considerably. Mersenne numbers, of the form 2^m — 1, are the most common examples. Pseudo-Mersenne numbers [5], generalized Mersenne numbers [14], and their extension [4] are other examples of numbers allowing fast modular arithmetic.

In a recent paper [2], we have defined the so-called Modular Number Systems (MNS) and Adapted Modular Number Systems (AMNS) to speed up the arithmetic operations for moduli which do not belong to any of the previous classes. In this paper, we propose a new representation, and the corresponding arithmetic operations for the elements of $\mathbb{Z}_p$, the ring of integers modulo p. (The integer p does not have to be a prime, although it is very likely to be prime for practical cryptographic applications.) We define the Polynomial Modular Number System (PMNS), over which integers are represented as polynomials. Compared to the classical (binary) representation, polynomial arithmetic offers the advantages of no carry propagation and easiest paral- lelization. The main

contribution of this paper is the fundamental theorem of a MNS, which provides a bound for the coefficients of the polynomials used to represent the elements of $\mathbb{Z}_p$. This theorem is presented in Section 3. It uses results from lattice reduction theory [9, 11]. The second half of the paper focuses on the arithmetic operations; in Section 4, we propose algorithms for the basic operations - addition, multiplication, conversions - which all require a final step, called coefficient reduction ,that we present in details in Section 5. A numerical example is provided in Section 6.

2. Modular number systems

In classic positional number systems, every non-negative integer, x, is uniquely represented in radix r as

$$x \quad \sum_{i \ 0}^{n \ 1} x_i r^i, \quad \text{where } x_i \in \{0, \ldots, r-1\}. \qquad (1)$$

If x_{n-1} =0, x is said to be a n-digit radix-r number.

In most public-key cryptographic applications, computations have to be done over finite rings or fields. In prime fields gf (p), we deal with representatives of equivalence classes modulo p (for simplicity we generally use the set of positive integers {0,1,...,p — 1}), and the arithmetic operations - addition and multiplication - are performed modulo p. In order to represent the set of integers modulo p, we define a Modular number system, by extending the Definition (1) of positional number systems.

Definition 1 (MNS) A Modular Number System, B, is a quadruple (p, n, γ, ρ), such that every positive integers, $0 \leq x < p$, satisfy

$$x \quad \sum_{i \ 0}^{n \ 1} x_i \gamma^i \bmod p, \quad with \ \gamma > 1 \ and \ |x_i| < \rho. \qquad (2)$$

The vector $(x_0,..., x_{n-1})_B$ denotes a representation of x in $\mathcal{B} \quad MNS(p, n, \gamma, \rho)$.

In the rest of the paper, we shall omit the subscript $(.)_B$ when it is clear from the context. We shall represent the integer, a, either as the vector, a, or the polynomial, A, without distinction. We shall use a_i to represent both for the ith element of a, and the ith coefficient of A. (Note that we use a left-to-right notation; i.e., a_0, the left-most coefficient of A, is the constant term.) Hence, depending on the context, we shall use $\|\boldsymbol{a}\| - \|A\|$, to refer to the norm of the vector, or the corresponding polynomial. We shall also use the notation ai to refer to the ith vector within a set of vectors or a matrix.

Example 1 Let us consider a MNS defined with p = $17, n - 3, \gamma - 7, \rho - 2.$ Over this system, we represent the elements of $\mathbb{Z}_{17}$ as polynomials in γ of degree at most 2, with coefficients in { — 1,0,1} (cf. table 1).

1	2	3	4
1	$-\gamma^2$	$1-\gamma^2$	$-1 \mid \gamma \mid \gamma^2$
5	6	7	8
$\gamma \mid \gamma^2$	$-1 \mid \gamma$	γ	$1 \mid \gamma$
9	10	11	12
$-1-\gamma$	$-\gamma$	$1-\gamma$	$-\gamma-\gamma^2$
13	14	15	16
$1-\gamma-\gamma^2$	$-1+\gamma^2$	γ^2	$1+\gamma^2$

Table 1. The elements of $\mathbb{Z}_{17}^*$ in the MNS defined as B = MNS (17, 3, 7, 2)

In example 1, we remark that the number of polynomials of degree 2, with coefficients in {—1,0,1} is equal to 3^3 = 27. Since we only have to represent 17 values, the system is clearly redundant. For example, we have $6 - 1 \mid \gamma \mid \gamma^2 - = -1 \mid \gamma$, or $9 - 1 - \gamma \mid \gamma^2 - -1 - \gamma$. The level of redundancy depends on the parameters of the MNS. Note yet that, in this paper, we shall take advantage of the redundancy only by considering different representations of zero.

In a MNS, every integer, $0 \leq x < p$, is thus represented as a polynomial in γ. But; what do we know about the

coefficients of those polynomials? Are they bounded by some value which depends on the parameters of the MNS? In other words, given the integers p and n, are we able we determine ρ and construct a MNS? We answer these questions in the next section. We prove the fundamental theorem of a MNS, using results from lattice reduction theory, and we introduce the concept of Polynomial Modular Number System (PMNS).

3. Polynomial Modular Number Systems

In this section, we consider special cases of modular number systems, where $\hat{\gamma}$ is a root (modulo p) of a given polynomial E. In the following fundamental theorem of a MNS, we prove that if ρ is greater than a certain bound, then it is always possible to define a valid MNS. Roughly speaking, Theorem 1 says that there exists a MNS, $\mathcal{B} = MNS(p, n, \gamma, \rho)$, where one can represent every integer less than p, as a polynomial of degree at most n — 1, with coefficients all less than C x $p^{1/n}$, where C is a small constant.

Theorem 1 (Fundamental theorem of a MNS) Let us define p,n > 1, and a polynomial $E(X) = X^n + \alpha X + \beta$, with $\alpha, \beta \in \mathbb{Z}$, such that $E(\gamma) \equiv 0 \pmod{p}$, and E irreducible in $\mathbb{Z}[X]$. If

$$\rho \geq (|\alpha| + |\beta|)\, p^{1/n}, \qquad (3)$$

then, the parameters (p, n, γ, ρ) define a modular number system, $\mathcal{B} = MNS(p, n, \gamma, \rho)$. Sketch of proof: (A complete, detailed, proof can be found in [1].)

The proof is based on the theory of lattice reduction [9, 11]. A lattice $\mathcal{L}$ is a discrete sub-group of $\mathbb{R}^n$, or equiv- alently the set of all the integral combinations of $d \leq n$ linearly independent vectors over $\mathbb{R}$:

$$\mathcal{L} = \mathcal{L}(\boldsymbol{A}) = \mathbb{Z}\,\boldsymbol{a}_1 + \cdots + \mathbb{Z}\,\boldsymbol{a}_d = \{\lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_n \boldsymbol{a}_d \,;\, \lambda_i \in \mathbb{Z}\}.$$

The matrix A = (a_1,..., a_d) is called a basis of $\mathcal{L}$. It is known that, every vector over $\mathbb{R}$ can be reduced, modulo the lattice, within the fundamental domain of $\mathcal{L}$, given by

$$\mathcal{H} = \{x \in \mathbb{R}^n \,;\, x = \sum_{i=1}^{d} x_i\, \boldsymbol{a}_i,\ 0 \leq x_i < 1\}.$$

In order to prove Theorem 1, we first define the lattice, $\mathcal{L} = \mathcal{L}(\boldsymbol{A})$, over $\mathbb{Z}^n$, of all the multiples of p in B; or equivalently, the set of vector of $\mathbb{Z}^n$ defined by

$$\mathcal{L} = \mathcal{L}(\boldsymbol{A}) = \{(x_0, \ldots, x_{n-1}) : x_0 + x_1\gamma + \cdots + x_{n-1}\gamma^{n-1} \equiv 0 \pmod{p}\}. \qquad (4)$$

From Minkowski's theorem [9, 7], and because we have $|\det \boldsymbol{A}| = p$, we prove that there exists a vector $\boldsymbol{v} \in \mathcal{L}$, such that $\|\boldsymbol{v}\|_\infty \leq p^{1/n}$. We then define a second lattice, $\mathcal{L}'$ $\mathcal{L}'(\boldsymbol{B}) \subseteq \mathcal{L}$, of dimension n, with B=(b_1,..., b_n),

such that

$$\|\boldsymbol{b}_i\|_\infty \leq (|\alpha| + |\beta|)\, p^{1/n}. \qquad (5)$$

To conclude the proof, we simply remark that every integer, $a \in \mathbb{N}$, can be first associated with the vector a = (a, 0,..., 0), and reduced modulo $\mathcal{L}'$ to a vector $\boldsymbol{a}'$, which belongs to the fundamental domain $\mathcal{H}'$ of $\mathcal{L}'$. Since $\mathcal{H}'$ can be overlapped by spheres of radius $(|\alpha| + |\beta|)\, p^{1/n}$, and centers the vertices of $\mathcal{H}'$, and because all the points of a lattice are equivalent, we conclude that $\|\boldsymbol{a}'\|_\infty \leq (|\alpha| + |\beta|)\, p^{1/n}$.

Definition 2 (PMNS) A modular number system $\mathcal{B} = MNS(p, n, \gamma, \rho)$ which satisfies the conditions of Theorem 1 is called a Polynomial Modular Number

System (PMNS). We shall denote $\mathcal{B} = PMNS(p, n, \gamma, \rho, E)$. In practice, we shall define the polynomial E with α and β as small as possible.

Example 2 We define the PMNS with $p = 23, n = 3, \rho = 2, E(X) - X^3 - X + 1\ (\alpha - -1, \beta - 1)$. We easily check that γ = 13 is a root of E in $\mathbb{Z}_{23}$, and E is irreducible in $\mathbb{Z}[X]$. We represent the elements of $\mathbb{Z}_{23}$ as polynomials of degree at most 2, with coefficients in { — 1,0,1}.

4. Conclusions

In this paper, we have proposed a new representation for the elements of Z_p, the ring of integers modulo p, called Polynomial Modular Number Systems. In this system, integers are represented as polynomials in 7, of degree less than n, with coefficients bounded by $(|a| + |ft|)p^{1/n}$, where a, ft are very small integers. Since $p^{1/n}$ is a minimum value,

R_i	$r_{i,0}$	$r_{i,1}$	$r_{i,2}$	$r_{i,3}$
R_{13}	13976766	−84549634	−24162638	−26689282
R_{12}	14488766	−24305666	−20345166	−32534274
R_{11}	13759678	−9254914	−620878	−17989378
R_{10}	4661438	−2222082	1705650	−1809154
R_9	1237182	−2060802	1175730	−1774850
R_8	1237182	−2060802	1175730	−1774850
R_7	323390	−895874	−54222	−975362
R_6	247870	−310274	−70670	−395842
R_5	210110	−17474	−78894	−106082
R_4	103102	−12434	−95454	−105010
R_3	46214	−4626	−24166	−55938
R_2	7958	−6282	−26850	−22402
R_1	7130	−7624	−10082	−3274
R_0	6095	−7557	−3394	−3589

Table 2. The iterations performed by the CTCR Algorithm 3

only a few extra bits are required for each coefficient. Compared to the classic multiprecision representation, the polynomial nature of PMNS allows for no-carry propagation, and efficient polynomials arithmetic. The algorithms presented in this paper for the arithmetic operations must be seen as a first step in doing the arithmetic over this new representation. Many improvements are still to come...

References

1. J.-C. Bajard, L. Imbert, and T. Plantard. Arithmetic operations in the polynomial modular number system. Research Report 04030, LIRMM - CNRS, 161 rue Ada, 34392 Mont- pellier cedex 5, France, Sept. 2004. Available electronicaly at http://www.lirmm.fr/~imbert.

2. J.-C. Bajard, L. Imbert, and T. Plantard. Modular number systems: Beyond the Mersenne family. In Selected Areas in Cryptography: 11th International Workshop, SAC 2004, volume 3357 of LNCS, pages 159-169. Springer-Verlag, Jan. 2005.

3. P. Barrett. Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In A. M. Odlyzko, editor, Advances in Cryptol- ogy - CRYPTO '86, volume 263 of LNCS, pages 311-326. Springer-Verlag, 1986.

4. J. Chung and A. Hasan. More generalized mersenne numbers. In M. Matsui and R. Zuccherato, editors, Selected Areas in Cryptography - SAC 2003, volume 3006 of LNCS, pages 335-347. Springer-Verlag, 2004.

5. R. Crandall. Method and apparatus for public key exchange in a cryptographic system. U.S. Patent number 5159632, 1992.

6. W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT- 22(6):644-654, November 1976.

7. C. Dwork. Lattices and their applications to cryptography. Lecture notes, Stanford University, 1998.

8. D. Hankerson, A. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004.

9. L. Lovasz. An Algorithmic Theory of Numbers, Graphs and Convexity, volume 50 of CBMS-NSF Regional Conference Series in Applied Mathematics. SIAM Publications, 1986.

10. A. Menezes, P. C. Van Oorschot, and S. A. Vanstone. Handbook of applied cryptography. CRC Press, 1997.

11. D. Micciancio and S. Goldwasser. Complexity of Lattice Problems, A Cryptographic Perspective. Kluwer Academic Publishers, 2002.

12. P. L. Montgomery. Modular multiplication without trial division. Mathematics of Computation, 44(170):519-521, Apr. 1985.

13. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2):120-126, February 1978.