NTRU Algebra Tutorial

Here you will find information about the algebraic structures which are used in NTRU's cryptographic product

1. MODULAR ARITHMETIC

Modular arithmetic is simply division with remainder, where you keep the remainder and throw everything else away. For example, the expression

147 (modulo 17)

means to divide 147 by 17 and keep the remainder. Now 147 divided by 17 gives a quotient of 8 and a remainder of 11 (since 147 = 8 × 17 + 11), so 147 (modulo 17) is equal to 11. This is written as an equality (called a congruence)

147 = 11 (modulo 17).

In general, the expression

a (modulo m)

means to divide a by m and keep the remainder. Similarly, a congruence

a = b (modulo m)

simply means that a and b leave the same remainder when they are divided by m. This is the same as saying that the difference a-b is a multiple of m. The integer m is called the modulus of the congruence.

Numbers and congruences with the same modulus may be added, subtracted, and multiplied just as is done with ordinary equations. For example,

(8 modulo 23) + (6 modulo 23) = 14 modulo 23, and

(8 modulo 23) × (6 modulo 23) = 48 modulo 23 = 2 modulo 23.

If a and m have no common factors, then it is also possible to find an inverse for a (modulo m), that is, to find an integer b so that

a × b = 1 (modulo m).

For example, the inverse of 10 (modulo 23) is 7, since 7×10=70=1 (modulo 23). There is a very fast algorithm, called the Euclidean algorithm, which can be used to check if a and m have common factors and also to compute the inverse of a (modulo m) if they do not have common factors. A description of the Euclidean algorithm may be found in any standard number theory textbook. (For example, see [Cohen, Section 1.3] or [Silverman, Chapters 5 and 6].)

2. TRUNCATED POLYNOMIAL RINGS

The principal objects used by the NTRUEncrypt PKCS are polynomials of degree N-1 having integer coefficients:

$$\mathbf{a} = a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}.$$

The coefficients $a_0,\ldots,a_{N-1}$ are integers. Some of the coefficients are allowed to be 0.

The set of all such polynomials is denoted by **R**. The polynomials in **R** are added together in the usual way by simply adding their coefficients:

$$\mathbf{a} + \mathbf{b} = (a_0+b_0) + (a_1+b_1)X + \ldots + (a_{N-1}+b_{N-1})X^{N-1}.$$

They are also multiplied in almost the usual manner, with one change. After doing the multiplication, the power X^N should be replaced by 1, the power X^{N+1} should be replaced by X, the power X^{N+2} should be replaced by X^2, and so on.

Example. Suppose N=3, and take the two polynomials **a**=2-X+3X^{2}and **b**=1+2X-X^2. Then

$$\mathbf{a} + \mathbf{b} = (2-X+3X^2) + (1+2X-X^2) = 3+X+2X^2 \text{ and}$$

$$\mathbf{a}*\mathbf{b} = (2-X+3X^2)*(1+2X-X^2) = 2+3X-X^2+7X^3-3X^4 = 2+3X-X^2+7-3X = 9-X^2.$$

The following is the general formula for multiplying polynomials in **R**:

$$\mathbf{a}*\mathbf{b} = c_0 + c_1X + c_2X^2 + c_3X^3 + \ldots + c_{N-2}X^{N-2} + c_{N-1}X^{N-1},$$

where the kth coefficient ck is given by the formula

$$c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 + a_{k+1}b_{N-1} + a_{k+1}b_{N-2} + \ldots a_{N-1}b_{k+1}.$$

This formula looks a little complicated, but it really isn't. The kth coefficient c_k is simply the dot product of the coefficients of **a** and the coefficients of **b**, except that first the coefficients of **b** are listed in reverse order and are rotated around k positions.

Using these addition and multiplication rules, all of the familiar properties are true. For example, the distributive law,

$$\mathbf{a}*(\mathbf{b}+\mathbf{c}) = \mathbf{a}*\mathbf{b} + \mathbf{a}*\mathbf{c}$$

is true. In modern terminology, the above addition and multiplication rules make **R** into a ring, which we call the Ring of Truncated Polynomials. In terms of modern abstract algebra, the ring **R** is isomorphic to the quotient ring **Z**[X]/(X^N-1).

Example. Here's a larger example with N=7, **a**=3+2X^2-3X^4+X^6, **b**=1-3X+X^2+2X^5-X^6. Then

a + b = 4 - 3X + 3X^2 - 3X^4 + 2X^5,
a*b = 4 - 10X - X^2 - 3X^3 + X^4 + 14X^5 - 5X^6.

The NTRUEncrypt PKCS uses the ring of truncated polynomials **R** combined with the modular arithmetic described in Section 1. These are combined by reducing the coefficients of a polynomial **a** modulo an integer q. Thus the expression

a (modulo q)

means to reduce the coefficients of **a** modulo q. That is, divide each coefficient by q and take the remainder.

Similarly, the relation

$$\mathbf{a} = \mathbf{b} \text{ (modulo q)}$$

means that every coefficient of the difference **a-b** is a multiple of q.

Remark. To make storage and computation easier, it is convenient to just list the coefficients of a polynomial without explicitly writing the powers of X. For example, the polynomial

$$\mathbf{a} = a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$$

is conveniently written as the list of N numbers

$\mathbf{a} = (a_0, a_1, a_2, \ldots ,, a_{N-2}, a_{N-1})$.

Be sure to include zeros in the list if some of the powers of X are missing. For example, when N=7 the polynomial $\mathbf{a}=3+2X^2-3X^4+X^6$ is stored as the list (3,0,2,0,-3,0,1). But if N=9, then a would be stored as the list (3,0,2,0,-3,0,1,0,0).

3. INVERSES IN TRUNCATED POLYNOMIAL RINGS

The inverse modulo q of a polynomial a is a polynomial A with the property that

$\mathbf{a*A} = 1$ (modulo q).

Not every polynomial has an inverse modulo q, but it is easy to determine if a has an inverse, and to compute the inverse if it exists. A fast algorithm for computing the inverseis described in NTRU Technical Note 014, and a theoretical discussion of inverses in truncated polynomial rings is given in NTRU Technical Note 009. These notes may be downloaded from the Technical Center.

Example. Take N=7, q=11, $\mathbf{a}=3+2X^2-3X^4+X^6$. The inverse of a modulo 11 is $\mathbf{A}=-2+4X+2X^2+4X^3-4X^4+2X^5-2X^6$, since

$(3+2X^2-3X^4+X^6)*(-2+4X+2X^2+4X^3-4X^4+2X^5-2X^6) = -10+22X+22X^3-22X^6 = 1$ (modulo 11).