NTRU Cryptosystems Technical Report

Report # 8, Version 1
Title: Efficient Conversions from Mod $q$ to Mod $p$
Author: Joseph H. Silverman
Release Date: Tuesday, September 22, 1998

*Abstract.* An efficient method for converting a list of numbers modulo $q$ to a list of numbers modulo $p$ is described.

Various telecommunications protocols require the conversion of a list of numbers modulo $q$ into a list of numbers modulo $p$. For example, one might want to convert a list of bits ($q = 2$) or bytes ($q = 2^8 = 256$) into a list of "trits" ($p = 3$). The general fact governing such conversions is the following:

**Mod $q$ to Mod $p$ Conversion Algorithm**. *Suppose that $m$ and $n$ are integers such that*

$$q^m < p^n.$$

*Let $\alpha = [\alpha_0, \ldots, \alpha_{m-1}]$ be a list of $m$ numbers modulo $q$; that is, $0 \le \alpha_i < q$. Then $\alpha$ can be uniquely converted into a list of $n$ numbers modulo $p$,*

$$\beta = [\beta_0, \ldots, \beta_{n-1}], \qquad 0 \le \beta_i < p,$$

*according to the formula*

$$\sum_{i=0}^{m-1} \alpha_i q^i = \sum_{i=0}^{n-1} \beta_i p^i.$$

*The $\beta_i$'s can be computed from the $\alpha_i$'s using repeated division (by $p$) with remainder. Conversely, if one is given the $\beta_i$'s, then one can recover the $\alpha_i$'s by repeated division (by $q$) with remainder.*

The *efficiency* of storing $m$ numbers modulo $q$ in a list of $n$ numbers modulo $p$ is measured by the quantity

$$E(q, m; p, n) = \frac{\log q^m}{\log p^n}.$$

The closer $E(q, m; p, n)$ is to 1, the more efficient the conversion. Thus efficient conversions may be found by looking for fractions $m/n$ for which the difference

$$\frac{\log p}{\log q} - \frac{m}{n}$$

is positive and as small as possible. In general, the ratio $\log p/\log q$ will be irrational (indeed, transcendental). The theory of continued fractions tells us how to find the rational numbers which most closely approximate a given irrational number. For basic information about continued fractions, see [1, chapter IV] or [2, chapter X].

*Example.* Mod 2 to Mod 3 Conversion

We begin with the continued fraction expansion

$$\frac{\log 3}{\log 2} = 1.5849625\ldots = [1,1,1,2,2,3,1,5,2,23,\ldots].$$

The first few convergents (i.e., taking the first few terms) satisfying the required inequality are

$$\frac{\log 3}{\log 2} \approx \frac{3}{2}, \frac{19}{12}, \frac{84}{53}, \frac{1054}{665}.$$

These give efficiencies

$$E(2,3;3,2) = 94.64\%, \qquad E(2,19;3,12) = 99.897\%,$$
$$E(2,84;3,53) = 99.9964\%, \qquad E(2,1054;3,665) = 99.999994\%.$$

Thus for example, it is possible to store 19 bits in 12 trits with almost 99.9% efficiency; and one can store 84 bits in 53 trits with better than 99.996% efficiency. These two examples are thus good choices for most applications.

To indicate how good these approximations are in an absolute (as opposed to logarithmic) sense, we note that

$$\frac{2^{19}}{3^{12}} = \frac{524288}{531441} = 0.98654\ldots,$$
$$\frac{2^{84}}{3^{53}} = \frac{19342813113834066795298816}{19383245667680019896796723} = 0.99791\ldots.$$

*Example.* Mod 256 to Mod 3 Conversion

The continued fraction expansion of $\log 3/\log 256$ is

$$\frac{\log 3}{\log 256} = 0.19812031259\ldots = [0,5,21,12,2,11,2,\ldots].$$

The first few convergents smaller than $\log 3/\log 256$ are

$$\frac{\log 3}{\log 256} \approx \frac{21}{106}, \frac{527}{2660}, \frac{12627}{63734}.$$

For practical purposes, one would probably use the first of these, which says that 21 bytes fits into 106 trits with efficiency

$$E(256,21;3,106) = 99.99641\%.$$

On an absolute scale, we see that $256^{21}$ and $3^{106}$ are really quite close to one another:

$$256^{21} = 374144419156711147060143317175368453031918731001856$$
$$3^{106} = 375710212613636260325580163599137907799836383538729$$
$$\frac{2^{168}}{3^{106}} = 0.99583\ldots$$

For large amounts of data, one could use the next approximation and convert blocks of 527 bytes into 2660 trits with an efficiency virtually indistinguishable from 100%.

## References


[1] H. Davenport, *The Higher Arithmetic*, 4th edition, Hutchinson & Co., 1970.

[2] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, 4th edition, Oxford University Press, 1960.


---


Comments and questions concerning this technical report should be addressed to

`techsupport@ntru.com`

Additional information concerning NTRU Cryptosystems and the NTRU Public Key Cryptosystem are available at

`www.tiac.net/users/ntru`


---


NTRU is a trademark of NTRU Cryptosystems, Inc.

The NTRU Public Key Cryptosystem is patent pending.

The contents of this technical report are copyright Tuesday, September 22, 1998 by NTRU Cryptosystems, Inc.