NTRU Cryptosystems Technical Report

Report # 009, Version 1

Title: Invertibility in Truncated Polynomial Rings

Author: Joseph H. Silverman

Release Date: Thursday, October 1, 1998

Abstract. Let $R_q = (\mathbf{Z}/q\mathbf{Z})[X]/(X^N - 1)$ be the ring of truncated polynomials modulo q. We compute the probability that a randomly chosen polynomial $f(X) \in R_q$ is invertible in R_q, and also the conditional probability if $f(X)$ is required to satisfy $f(1) = 1$.

§1. Statements.

Fix an integer $N \geq 2$. For any positive integer q, let R_q denote the ring of truncated polynomials modulo q,

$$R_q = (\mathbf{Z}/q\mathbf{Z})[X]/(X^N - 1).$$

In this note we will describe the group of units (i.e., invertible elements)

$$R_q^* = \{f \in R_q \,:\, fg = 1 \text{ for some } g \in R_q\}.$$

More precisely, we are interested in the probability that an element of R_q is invertible, so in the ratio $\#R_q^*/\#R_q$.

Our first observation is that if $q = q_1 q_2$ with $(q_1, q_2) = 1$, then the Chinese Remainder Theorem tells us that

$$R_q = R_{q_1} \times R_{q_2} \quad \text{and} \quad R_q^* = R_{q_1}^* \times R_{q_2}^*,$$

so it suffices to look at the case that q is a power of a prime p. The following theorem handles this case.

Theorem A. *Let p be a prime, let $q = p^k$ be a power of p, and let $N \geq 2$ be an integer with $\gcd(p, N) = 1$. Define $n \geq 1$ to be the smallest positive integer such that*

$$p^n \equiv 1 \pmod{N},$$

and for each integer $d | n$, let

$$\nu_d = \frac{1}{d} \sum_{e|d} \mu\left(\frac{d}{e}\right) \gcd(N, p^e - 1). \tag{1}$$

Then

$$\frac{\#R_q^*}{\#R_q} = \prod_{d|n} \left(1 - \frac{1}{p^d}\right)^{\nu_d}. \tag{2}$$

In particular, if N is prime, then $\nu_d = 0$ for all $1 < d < n$, so in this case

$$\frac{\#R_q^*}{\#R_q} = \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^n}\right)^{(N-1)/n}. \tag{3}$$

Remark B. There is a certain set of non-invertible elements which is easy to describe. To do this, we observe that the evaluation map

$$R_q \longrightarrow \mathbf{Z}/q\mathbf{Z}, \qquad f(X) \longmapsto f(1)$$

is a well defined homomorpism of rings, so it induces a group homomorphism $R_q^* \to (\mathbf{Z}/q\mathbf{Z})^*$. It is well-known that

$$(\mathbf{Z}/q\mathbf{Z})^* \cong \{a \in \mathbf{Z}/q\mathbf{Z} \,:\, \gcd(a,q) = 1\},$$

so we see that if $f(1)$ has a factor in common with q, then it cannot be invertible. Thus in looking for invertible elements of R_q, we should make our "random" selection intelligently by requiring that $\gcd(f(1), q) = 1$. In particular, we must avoid polynomials with $f(1) = 0$.

For example, we might restrict attention to the subsets of R_q and R_q^* consisting of polynomials $f(X)$ satisfying $f(1) = 1$. We denote these subsets by $R_q(1)$ and $R_q^*(1)$ respectively.

As f ranges over R_q, the values of $f(1)$ are equidistributed in $\mathbf{Z}/q\mathbf{Z}$, so we see that $\#R_q(1) = q^{-1}\#R_q$. Similarly, as f ranges over R_q^*, the values of $f(1)$ are equidistributed in $(\mathbf{Z}/q\mathbf{Z})^*$, so $\#R_q^*(1) = \phi(q)^{-1}\#R_q^*$, where ϕ is the Euler phi function. In particular, if $q = p^k$ is a power of a prime, then $\phi(q) = p^k - p^{k-1}$ and we find that the probability of an "intelligently chosen" f being invertible is

$$\frac{\#R_q^*(1)}{\#R_q(1)} = \left(1 - \frac{1}{p}\right)^{-1} \frac{\#R_q^*}{\#R_q}.$$

Since p tends to be small in applications, this is a significant savings. For example, if we also assume that N is prime, then

$$\frac{\#R_q^*(1)}{\#R_q(1)} = \left(1 - \frac{1}{p^n}\right)^{(N-1)/n} \approx 1 - \frac{N-1}{np^n}.$$

Remark C. It is clear from Theorem A that in order to maximize the probability of getting a unit in R_q, we want to choose N and p so that the order n of p in $(\mathbf{Z}/N\mathbf{Z})^*$ is as large as possible. The value of n is easy to compute for specific values of N and p, but for cryptographic purposes we will want n to be large for a single N and two different values of p (frequently $p = 2$ and $p = 3$). Notice that the possible orders of elements in $(\mathbf{Z}/N\mathbf{Z})^*$ are the divisors of $\phi(N)$, so if we take N to be prime, the possible orders are divisors of $N-1$. This suggests choosing N to be a prime such that $N-1$ has very few divisors.

For example, suppose that N is a prime of the form $N = 2M+1$ with M also prime. (The prime M is called a Sophie Germain prime.) Then the divisors of $N-1$ are 1, 2, M, and $2M$. So if N does not divide p^2-1, then the corresponding n must be either M or $2M$. In particular, if we take $N > 100$, then every primes $p < 10$ has corresponding $n = M$ or $2M$, and hence the probability that a randomly chosen f satisfying $f(1) = 1$ will be invertible is at least

$$1 - \frac{N-1}{Mp^M} = 1 - \frac{2}{p^M}.$$

Since $p \geq 2$ and $M \geq 50$, the probability of choosing a non-invertible polynomial is virtually 0.

§2. Examples.

Table 1 gives some representative values of N and p. The column labeled n_p gives the smallest integer n such that

$$p^n \equiv 1 \pmod{N}.$$

The column labeled "Prob$_p$" is the probability that a randomly chosen $f(X)$ in R_q satisfying $f(1) = 1$ will fail to be invertible in R_q, where $q = p^k$ is any power of p. (Theorem A and Remark B show that these probabilities are independent of the exponent k.) The values $N = 47, 59, 107, 167, 503, 1019$ (highlighted in the table) correspond to the Sophie Germain primes $(N-1)/2 = 23, 29, 53, 83, 251, 509$, and thus have especially small probability of failure for all (small) primes p. Conversely, $p = 2$ has order 7 modulo $N = 127$, and $p = 3$ has order 7 modulo $N = 1093$, so for these values of p and N, the ring R_p has a comparatively large number of non-units.

§3. Proof of Main Theorem.

In this section we will give the proof of Theorem A. We start with the following generalization of [1, Chapter 7, Section 2, Theorem 1].

Theorem 3.1. *Fix a prime p and an integer $N \geq 1$ satisfying $\gcd(N,p) = 1$. For any integer $d \geq 1$, let $F_d(X)$ be the product of all monic irreducible polynomials in $\mathbf{F}_p[X]$ of degree d which divide $X^{N+1} - X$. Then for any integer $D \geq 1$,*

$$\prod_{d|D} F_d(X) = X^{(N,p^D-1)+1} - X. \tag{4}$$

Proof. For convenience we let $F(X)$ denote the polynomial on the lefthand side of (4) and $G(X)$ denote the polynomial on the righthand side. The polynomial $F(X)$

N	p	n_p	Prob_p		N	p	n_p	Prob_p
47	2	23	$10^{-7.22}$		**47**	3	23	$10^{-11.27}$
59	2	58	$10^{-17.46}$		**59**	3	29	$10^{-14.14}$
71	2	35	$10^{-10.84}$		71	3	35	$10^{-17.00}$
107	2	106	$10^{-31.91}$		**107**	3	53	$10^{-25.59}$
127	2	7	$10^{-3.36}$		127	3	126	$10^{-60.12}$
167	2	83	$10^{-25.29}$		**167**	3	83	$10^{-39.90}$
229	2	76	$10^{-23.36}$		229	3	57	$10^{-27.80}$
349	2	348	$10^{-104.76}$		349	3	174	$10^{-83.32}$
503	2	251	$10^{-75.86}$		**503**	3	251	$10^{-120.06}$
1019	2	1018	$10^{-306.45}$		**1019**	3	509	$10^{-243.16}$
1093	2	364	$10^{-110.05}$		1093	3	7	$10^{-5.53}$

Table 1. Probability $f(X)$ Is Not Invertible In R_{p^k}

is separable (i.e., has no multiple roots) by definition. The same is true of $G(X)$, since in general

$$\mathrm{Disc}(X^{K+1} - X) = \pm K^K,$$

and clearly $(N, p^D - 1) \neq 0$ in $\mathbf{F}_p$. It thus suffices to show that the (non-zero) roots of F and G coincide.

First let $\alpha \neq 0$ be a root of $F(X)$, say $F_d(\alpha) = 0$. This means that α generates an extension of $\mathbf{F}_p$ of degree d, and hence

$$\alpha^{p^d - 1} = 1.$$

On the other hand, by definition $F_d(X)$ divides $X^N - 1$, so every root of $F_d(X)$ satisfies $\alpha^N = 1$. Therefore

$$\alpha^{(N, p^d - 1)} = 1.$$

Further, we know that $d|D$, and so $p^d - 1$ divides $p^D - 1$, which implies that

$$\alpha^{(N, p^D - 1)} = 1.$$

Therefore $G(\alpha) = 0$.

Next let $\beta \neq 0$ be a root of $G(X)$, so $\beta^{(N, p^D - 1)} = 1$. Let d be the degree of β over $\mathbf{F}_p$, or equivalently, d is the smallest integer so that

$$\beta^{p^d} = \beta.$$

It follows that

$$\beta^{(N,p^D-1,p^d-1)} = 1,$$

and hence

$$\beta^{(p^D-1,p^d-1)} = 1.$$

It follows from [1, Chapter 7, Section 1, Lemma 3] that

$$(p^D-1,p^d-1) = p^{(D,d)}-1,$$

so

$$\beta^{p^{(D,d)}-1} = 1.$$

It follows from the minimality of d that $(D,d)=d$, and hence that $d|D$. We have proven that the degree d of β divides D, and hence that β is the root of $F_d(D)$ for some d dividing D. Therefore $F(\beta)=0$.

This completes the proof that $F(X)$ and $G(X)$ have the same roots, and hence that $F(X)=G(X)$. QED

Corollary 3.2. *With notation as above, let n and ν_d be defined as in the statement of Theorem A. Then*

$$R_p = \frac{\mathbf{F}_p[X]}{(X^N-1)} \cong \prod_{d|n} \left(\mathbf{F}_{p^d}\right)^{\nu_d}.$$

In particular,

$$\frac{\#R_p^*}{\#R_p} = \prod_{d|n}\left(1-\frac{1}{p^d}\right)^{\nu_d}.$$

Proof. If we factor X^N-1 into a product of irreducible polynomials in $\mathbf{F}_p[X]$,

$$X^N-1 = f_1(X)f_2(X)\cdots f_s(X),$$

then the Chinese Remainder Theorem tells us that

$$\mathbf{F}_p[X]/(X^N-1) \cong \frac{\mathbf{F}_p[X]}{(f_1(X))}\times\cdots\times\frac{\mathbf{F}_p[X]}{(f_s(X))} \cong \mathbf{F}_{p^{\deg(f_1)}}\times\cdots\times\mathbf{F}_{p^{\deg(f_s)}}.$$

(Note that $f_1,\ldots,f_s$ are necessarily distinct since $\gcd(N,p)=1$ ensures that X^N-1 is separable.) Hence if we let

$$\lambda_d = \#(\text{irreducible factors of } X^N-1 \text{ of degree } d),$$

then we have an isomorphism

$$\mathbf{F}_p[X]/(X^N-1) \cong \prod_d \left(\mathbf{F}_{p^d}\right)^{\lambda_d}.$$

To complete the proof of Corollary 3.2, it remains to show that λ_d is equal to ν_d.

To apply Theorem 3.1, we look instead at

$$\lambda'_d = \#(\text{irreducible factors of } X^{N+1} - X \text{ of degree } d),$$

so $\lambda'_1 = \lambda_1 + 1$, and $\lambda'_d = \lambda_d$ for $d > 1$. Then in the notation of Theorem 3.1, we have by definition

$$\deg F_d(X) = d\lambda'_d.$$

Taking the degree of both sides of equation (4) yields for any integer $D \geq 1$,

$$\sum_{d|D} d\lambda'_d = (N, p^D - 1) + 1.$$

Since this holds for all D, we can apply Möbius inversion to get

$$d\lambda'_d = \sum_{e|d} \mu\left(\frac{d}{e}\right) \big((N, p^e - 1) + 1\big).$$

(See, e.g., [1, Chapter 2, Section 2].) Since $\sum_{e|d} \mu(d/e) = 0$ for all $d > 1$, we find that

$$d\lambda_d = \sum_{e|d} \mu\left(\frac{d}{e}\right) (N, p^e - 1)$$

for all d, which gives the desired equality $\lambda_d = \nu_d$. This completes the proof of the first statement. For the second, we merely use the fact that the unit group of a product of rings is equal to the product of the unit groups, and hence

$$\#\left(\prod_{d|n} (\mathbf{F}_{p^d})^{\nu_d}\right)^* = \#\prod_{d|n} \left(\mathbf{F}^*_{p^d}\right)^{\nu_d} = \prod_{d|n} (p^d - 1)^{\nu_d}. \qquad \text{QED}$$

Notice that Corollary 3.2 completes the proof of formula (2) in Theorem A in the case that q is prime. It remains to show that the case of prime powers is essentially the same. We begin with a lemma which says that units modulo p can always be lifted to units modulo powers of p.

Lemma 3.3. *Let p be a prime, and let f be a polynomial. If f is a unit in R_p, then f is a unit in R_{p^k} for every $k \geq 1$.*

Proof. Since f is a unit in R_p, there is a polynomial g such that

$$fg \equiv 1 \pmod{p}.$$

We construct an inverse to f modulo higher powers of p inductively (using Newton iteration) as follows. Set $g_0 = g$. Then given g_i, set

$$g_{i+1} = 2g_i - fg_i^2.$$

We claim that $fg_i \equiv 1 \pmod{p^{2^i}}$. This is true for $i = 0$ by construction. Suppose it is true for i, so $fg_i = 1 + p^{2^i}h$ for some h. Then

$$fg_{i+1} = f(2g_i - fg_i^2) = 1 - (1 - fg_i)^2 = 1 - p^{2^{i+1}}h^2 \equiv 1 \pmod{p^{2^{i+1}}}. \qquad \text{QED}$$

We are now ready to complete the proof of Theorem A. We observe that if $f(X) \equiv 1 \pmod{p}$, then f is automatically a unit in R_{p^k} for every $k \geq 1$. To see this, we just write $f(X) = 1 - pg(X)$ for some polynomial $g(X)$ and expand using the geometric series

$$f(X)^{-1} = \bigl(1 - pg(X)\bigr)^{-1} \equiv 1 + pg(X) + p^2g(X)^2 + \cdots + p^{k-1}g(X)^{k-1} \pmod{p^k}.$$

Combining this observation with Lemma 3.3, we see that for any $k \geq 2$ there is an exact sequence

$$1 \longrightarrow \bigl(1 + pR_{p^{k-1}}\bigr) \longrightarrow R_{p^k}^* \longrightarrow R_p^* \longrightarrow 1,$$

and hence

$$\#R_{p^k}^* = p^{(k-1)N}\#R_p^*.$$

Since also $\#R_{p^k} = p^{kN} = p^{(k-1)N}\#R_p$, we have proven that

$$\frac{\#R_{p^k}^*}{\#R_{p^k}} = \frac{\#R_p^*}{\#R_p}.$$

Now Corollary 3.2 says that formula (2) in Theorem A is correct.

The second part of Theorem A deals with the case that N is prime. In this case, we have for any $e|n$,

$$(N, p^e - 1) = \begin{cases} 1 & \text{if } 1 \leq e < n, \\ N & \text{if } e = n. \end{cases}$$

Substituting into the formula (1) for ν_d yields

$$\begin{aligned} \nu_d &= \frac{1}{d}\sum_{e|d}\mu\left(\frac{d}{e}\right) + \begin{cases} 0 & \text{if } d < n, \\ N - 1 & \text{if } d = n. \end{cases} \\ &= \begin{cases} 1 & \text{if } d = 1, \\ 0 & \text{if } 1 < d < n, \\ N - 1 & \text{if } d = n. \end{cases} \end{aligned}$$

(If $d = n = 1$, then $\nu_1 = N$.) Now putting these values into the general formula (2) for $\#R_q^*/\#R_q$ gives the desired formula (3), which completes the proof of Theorem A. QED

References

[1] *A Classical Introduction to Modern Number Theory*, K. Ireland and M. Rosen, Springer-Verlag, New York, 1982.

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`
