Tatra Mt. Math. Publ. **25** (2002), 127–136

TATRA MOUNTAINS
Mathematical Publications

RING UNITS IN ITERATED CYCLIC EXTENSIONS, AND IN NTRU

Markus Schmidmeier

ABSTRACT. We develop a formula for the number of units in finite commutative rings which arise as iterated cyclic extensions. The formula depends only on the degree of the irreducible factors of certain polynomials with coefficients in a finite field. Examples of such rings include the domain $\mathbb{Z}_q[x]/(x^N - 1)$ which is used to encrypt messages in the public key cryptographic system NTRU. We recognize the known problem that the checksum of a message in the standard setup of NTRU is not protected and describe how this problem is handled in our internet implementation HERMES of NTRU.

In this paper we construct and count the units in finite commutative rings which are given as cyclic extensions. Our result can be applied to the study of the public key cryptographic system NTRU, which is based on the theory of finite commutative rings, and in which units play a key role, namely the role of *keys*. NTRU has attracted considerable interest recently as it is much faster than traditional public key systems and it appears to be secure since its security is based on, and perhaps equivalent to, the lattice basis reduction problem.

In the first section of the paper we study the units in finite commutative rings which are given as iterated cyclic extensions. Our formula for counting units starts at the innermost domain. For each extension, only the degrees of the irreducible factors of the defining polynomial with coefficients in a finite field are required.

In an application to NTRU in the following sections we point out that the checksum of a message modulo the "big" parameter q is not protected in the standard setup. We describe how this problem is avoided in our own implementation HERMES written in the internet language *JavaScript*.

2000 Mathematics Subject Classification: 13M10.
Keywords: ring, units, NTRU.

1. Counting units in finite commutative rings

Let k be a field, then the number of units of k is $|k^*| = |k| - 1$. Two generalizations give rise to the formula for the number of units in an arbitrary finite commutative ring R. First, assume that R is *local*, so R has a unique (proper) maximal ideal m, and the quotient ring $k = R/m$ is a field. For example, if $q = p^n$ is a prime power then the ring $\mathbb{Z}_q$, the integers mod q, is a local ring with maximal ideal the multiples of p (mod q). In each finite local ring, the maximal ideal m is a *nil* ideal, that is, the powers of any element in m eventually become zero. As a consequence of the following lemma, which is well known, we obtain that the number of units in R is

$$|R^*| = \big(|k| - 1\big) \cdot |m| = |R| \cdot \left(1 - \frac{1}{|k|}\right).$$

Lemma 1.1. *Let Λ be a finite ring, and $I \subset \Lambda$ a nil ideal. Then the number of units in Λ is*

$$|\Lambda^*| = \big|(\Lambda/I)^*\big| \cdot |I|.$$

More precisely, if $I = \{i_1, \ldots, i_n\}$, and if $\{u_1, \cdots, u_m\}$ is a set of representatives in Λ of the classes of the units in Λ/I, then Λ^* is the set

$$\Lambda^* = \{u_s + i_t \colon 1 \le s \le m,\ 1 \le t \le n\}.$$

Proof. Under the ring map $\Lambda \to \Lambda/I$, units go to units, and moreover, only units go to units: If $\bar{u}\bar{v} = 1$ holds in Λ/I and if u and v represent $\bar{u}$ and $\bar{v}$ in Λ then there is $i \in I$ such that $uv = 1 - i$ holds in Λ. This implies that $uv(1 + i + i^2 + i^3 + \cdots + i^{t-1}) = 1$ holds in Λ where t is the nilpotency index of i; so, u has a right inverse in Λ. $\square$

As any finite commutative ring R is a product of (finite) local rings, say $R = \prod_{i=1}^{n} R_i$ (see for example [1], Exercise 5, §27), the number of units in R is obtained as

$$|R^*| = |R_1^*| \cdot |R_2^*| \cdot \cdots \cdot |R_n^*| = |R| \cdot \left(1 - \frac{1}{|k_1|}\right) \cdots \left(1 - \frac{1}{|k_n|}\right)$$

where we denote by k_i the quotient field of R_i modulo its maximal ideal.

Example 1. For $q = 2$, the ring $R = \mathbb{Z}_q[T]/(T^7 - 1)$ is a product of three local rings, namely: Over $\mathbb{Z}_2$, the polynomial $f = T^7 - 1$ factors as a product of irreducible polynomials, $f = f_1 f_2 f_3$ where $f_1 = (T - 1)$, $f_2 = (T^3 + T + 1)$, and $f_3 = (T^3 + T^2 + 1)$. Thus, R is the product of three local rings, $R_1 \times R_2 \times R_3$ where $R_i = \mathbb{Z}_2[T]/(f_i)$ for each i. The Euclidean algorithm gives rise to a decomposition of 1 in R as $1 = (T^3) \cdot f_2 f_3 + (T^2+1) \cdot f_1 f_3 + (T^5+T^4) \cdot f_1 f_2$, so the ring inclusions $R_i \to R$ are given by multiplication by $e_i = h_i \cdot \prod\limits_{j \neq i} f_j$, where we have here $h_1 = T^3$, $h_2 = (T^2+1)$, and $h_3 = (T^5+T^4)$. Also, when considered as elements in R, the e_i form a full set of pairwise orthogonal idempotent elements in R. Note that multiplication by e_i defines a ring map $e_i \colon R_i \to R$; together with the canonical maps can_i, the maps e_i describe the direct product decomposition $R \cong \prod\limits_i R_i$, where R_i corresponds to the subring $e_i R$ in R.

$$\begin{tikzcd}
 & \frac{\mathbb{Z}_q[T]}{(f_1 f_2 f_3)} \arrow[dl, shift left, "\mathrm{can}_1"'] \arrow[dd, shift right, "\mathrm{can}_2"'] \arrow[dr, shift left, "\mathrm{can}_3"'] & \\
\frac{\mathbb{Z}_q[T]}{(f_1)} \arrow[ur, shift left, "e_1"'] & & \frac{\mathbb{Z}_q[T]}{(f_3)} \arrow[ul, shift left, "e_3"'] \\
 & \frac{\mathbb{Z}[T]}{(f_2)} \arrow[uu, shift right, "e_2"'] &
\end{tikzcd}$$

In our example, R is a product of three local rings (even fields), so the number of units in R is $|R^*| = 2^7 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{2^3}\right)^2$.

Next, we assume that for a base ring Λ the decomposition $\Lambda = \prod \Lambda_i$ as a product of local rings Λ_i, and the cardinalities of the rings Λ_i and of their maximal ideals $\mu_i \subset \Lambda_i$ are given. The aim is to specify the number of units in a cyclic extension R of Λ:

$$R = \frac{\Lambda[x]}{(p)}$$

where p is a monic polynomial with coefficients in Λ. We will see that the cardinality of the unit set in R can be computed easily from Λ provided only the irreducible factors of the classes of the polynomial p in certain finite fields are known.

First we handle the case that the base ring Λ is a local ring.

Lemma 1.2. *Let Λ be a local ring with maximal ideal μ and canonical map $\bar{\ } \colon \Lambda \to k = \frac{\Lambda}{\mu}$. Suppose that for a monic polynomial $f = \sum\limits_i a_i x^i$ in $\Lambda[x]$, the class of f in $k[x]$ factors as $\bar{f} = \sum\limits_i \bar{a}_i x^i = f_1^{m_1} \cdots f_n^{m_n}$ where the f_i are pairwise nonequivalent irreducible polynomials of degree $d_i = \deg f_i$. Then*

$$\left| \left(\frac{\Lambda[x]}{(f)} \right)^* \right| = \left| \frac{\Lambda[x]}{(f)} \right| \cdot \prod_{j=1}^{n} \left(1 - \frac{1}{|k|^{d_j}} \right).$$

P r o o f . The set $\frac{\mu[x]+(f)}{(f)}$ is a nil ideal in $\frac{\Lambda[x]}{(f)}$ with quotient

$$\frac{\frac{\Lambda[x]}{(f)}}{\frac{\mu[x]+(f)}{(f)}} = \frac{\Lambda[x]}{\mu[x]+(f)} = \frac{\frac{\Lambda[x]}{\mu[x]}}{\frac{\mu[x]+(f)}{\mu[x]}} = \frac{\frac{\Lambda}{\mu}[x]}{(\bar{f})},$$

thus, by Lemma 1.1, the number of units is $\left|\left(\frac{\Lambda[x]}{(f)}\right)^*\right| = \left|\frac{\mu[x]+(f)}{(f)}\right| \cdot \left|\left(\frac{\frac{\Lambda}{\mu}[x]}{(\bar{f})}\right)^*\right|$. In $\frac{\Lambda}{\mu}[x]$, $\bar{f}$ factors as $f_1^{m_1}\cdots f_n^{m_n}$, hence $\frac{k[x]}{(\bar{f})} = \frac{k[x]}{(f_1)^{m_1}} \times\cdots\times \frac{k[x]}{(f_n)^{m_n}}$, and each of the local rings $\frac{k[x]}{(f_j)^{m_j}}$ has $\left|\frac{k[x]}{(f_j)^{m_j}}\right| \cdot \left(1-\frac{1}{|k|^{d_j}}\right)$ units, again by Lemma 1.1. □

The lemma may look technical but it handles the rings that come up in the public key cryptographic system NTRU. Here, units occur in abundance:

COROLLARY 1.3. *Let $R = \mathbb{Z}_q[T]/(T^N-1)$ where $q = p^n$ is a prime power and N is such that the polynomial $T^N - 1$ factors over $\mathbb{Z}_p$ as a product of three factors, $T^N - 1 = f_1 f_2 f_3$, where $f_1 = T-1$ and where the two other irreducible factors f_2 and f_3 are not equivalent and have the same degree.*

1. *The probability that a random element in R is a unit is*

$$\frac{|R^*|}{|R|} = \left(1-\frac{1}{p}\right)\cdot\left(1-\frac{1}{p^{(N-1)/2}}\right)^2.$$

2. *The probability that a random element f in R which satisfies the extra condition that $f(1) = 1$, is a unit is*

$$\frac{|R^* \cap \{f\colon f(1)=1\}|}{|\{f\colon f(1)=1\}|} = \left(1-\frac{1}{p^{(N-1)/2}}\right)^2.$$

3. *Any non zero element $f\in R$ which has a polynomial representative of degree less than $(N-1)/2$ and which satisfies the extra condition that $f(1) = 1$, is always a unit.*

P r o o f . The first assertion is an application of Lemma 1.2. More directly, by Lemma 1.1, an element in R is a unit if and only if its class in the factor ring $\mathbb{Z}_p[T]/(T^N-1)$ modulo p is a unit. As in Example 1, this ring decomposes as a product of three fields, and we conclude that the number of units is as stated. For the second assertion, note that the condition that $f(1) = 1$ implies that the map can_1 in Example 1 maps f to the class of 1 in $\mathbb{Z}_q[T]/(T-1)$. There are exactly $|R|/q$ elements in R which satisfy the condition, and the same number of elements in R has the property that their class in $\mathbb{Z}_q[T]/(T-1)$ is 1 (indeed, there is exactly one value for the constant term so that the class of the element is 1). Hence a bijection between $R^*\cap\{f\colon f(1)=1\}$ and the product

$(\mathbb{Z}_q[T]/(f_2))^* \times (\mathbb{Z}_q[T]/(f_3))^*$ is given by the maps can_2 and can_3 so our claim is shown. Concerning the last assertion note that the condition $f(1) = 1$ ensures that $\mathrm{can}_1(f)$ is a unit while the degree requirement implies that also $\mathrm{can}_2(f)$ and $\mathrm{can}_3(f)$ are units. So, f is a unit. □

We now drop the assumption that Λ is a local ring.

Proposition 1.4. *Suppose $\Lambda = \prod \Lambda_i$ is a product of local rings (Λ_i, μ_i) with $\pi_i \colon \Lambda \to \Lambda_i$ the canonical projection onto the ith factor. Suppose that for a monic polynomial $f \in \Lambda[x]$, the class $\overline{\pi_i(f)}$ of f in $\frac{\Lambda_i}{\mu_i}$ factors as $\overline{\pi_i(f)} = f_{i1}^{n_{i1}} \cdots f_{is_i}^{n_{is_i}}$, where the polynomials f_{ij} have degree $\deg f_{ij} = d_{ij}$. Then*

$$\left|\left(\frac{\Lambda[x]}{(f)}\right)^*\right| = \prod_i \left|\left(\frac{\Lambda_i[x]}{(\pi_i(f))}\right)^*\right| = \left|\frac{\Lambda[x]}{(f)}\right| \prod_i \prod_{j=1}^{s_i}\left(1 - \frac{1}{|\frac{\Lambda_i}{\mu_i}|^{d_{ij}}}\right).$$

P r o o f. Suppose $\Lambda = \prod \Lambda_i$, then $\Lambda[x] = \prod \Lambda_i[x]$ and an ideal $I \subset \Lambda[x]$ has the form $I = \prod (I \cap \Lambda_i[x])$; in particular if $I = (f)$ where $f = \sum_{j=0}^{n} a_j x^j$ with $a_j = \sum_i a_{ji}$ and $a_{ji} \in \Lambda_i$ then $\pi_i(f) = \sum_j a_{ji} x^j$ and $(f) = \prod (\pi_i(f))$. Thus, $\frac{\Lambda[x]}{(f)} = \prod_i \frac{\Lambda_i[x]}{(\pi_i(f))}$, and the formula follows from Lemma 1.2 □

The following example shows that for iterated cyclic extensions, the number of units can be computed by working from the inside out.

Example 2. We compute the number of units in the ring $R = \frac{\mathbb{Z}_8[x]}{(x^7-1)} \frac{[y]}{(y^{63}-1)}$. We only use the following factorizations (see [2] and [3] for an account on factoring cyclotomic polynomials): As seen in Example 1, the polynomial $(x^7 - 1)$ factors over $\mathbb{Z}_2$ as $(x+1)(x^3+x^2+1)(x^3+x+1)$; the irreducible factors of $(y^{63}-1)$ in $\mathbb{Z}_2$ have degree as given in the formula $63 = 1 + 2 + 2\cdot 3 + 9 \cdot 6$; the same polynomial $(y^{63}-1)$ in $\mathbb{F}_8$ has 7 linear factors and 28 irreducible quadratic factors, all pairwise non-equivalent. Thus

$$\begin{aligned}
|R^*| &= \left|\left(\frac{\mathbb{Z}_8[x]}{(x^7-1)} \frac{[y]}{(y^{63}-1)}\right)^*\right| \\
&= \left|\left(\frac{\mathbb{Z}_2[x]}{(x^7-1)} \frac{[y]}{(y^{63}-1)}\right)^*\right| \cdot |(2)| \\
&= \left|\left(\frac{\mathbb{Z}_2[x]}{(x-1)} \frac{[y]}{(y^{63}-1)}\right)^*\right| \cdot \left|\left(\frac{\mathbb{Z}_2[x]}{(x^3+x^2+1)} \frac{[y]}{(y^{63}-1)}\right)^*\right| \cdot \\
&\quad \cdot \left|\left(\frac{\mathbb{Z}_2[x]}{(x^3+x+1)} \frac{[y]}{(y^{63}-1)}\right)^*\right| \cdot 2^{2\cdot 7\cdot 63}
\end{aligned}$$

$$
\begin{aligned}
&= \left| \left(\frac{\mathbb{Z}_2[y]}{(y^{63}-1)} \right)^* \right| \cdot \left| \left(\frac{\mathbb{F}_8[y]}{(y^{63}-1)} \right)^* \right|^2 \cdot 2^{2\cdot 7\cdot 63} \\
&= 2^{63} \cdot \left(1-\frac{1}{2}\right) \cdot \left(1-\frac{1}{2^2}\right) \cdot \left(1-\frac{1}{2^3}\right)^2 \cdot \left(1-\frac{1}{2^6}\right)^9 \\
&\qquad \cdot 8^{2\cdot 63} \cdot \left(1-\frac{1}{8}\right)^{2\cdot 7} \cdot \left(1-\frac{1}{8^2}\right)^{2\cdot 28} \cdot 2^{2\cdot 7\cdot 63}.
\end{aligned}
$$

2. Units in NTRU and the message checksum

Ring units play a key role in the public key cryptographic system NTRU, and in our internet application HERMES. In particular, we want to pick elements in the domain

$$\mathbb{Z}_3[T]/(T^N - 1)$$

which have a high probability of being a unit: First, the private key f itself has to be a unit, more precisely, it has to be such that its class in two quotients is a unit. Second, in the public key, one of the two units given by f is protected in HERMES by multiplication by another unit. Next, a message is protected by blinding it with the product of the public key and a unit. Finally, only a protected version of the private key is stored. For protection in HERMES we multiply f by a unit which is computed from a passphrase. In this section we recall quickly how messages are encrypted in NTRU and point out that in the standard version of NTRU, the checksum of a message is not protected; we describe how this problem is settled in HERMES.

Notation. For q a prime power, the canonical map modulo q, $\mathrm{mod}_q \colon \mathbb{Z} \to \mathbb{Z}_q$, is onto but not injective, so it has a right inverse, but this is not determined uniquely. By $\mathrm{sym}_q \colon \mathbb{Z}_q \to \mathbb{Z}$ we denote the set map which which maps $\bar{x} \in \mathbb{Z}_q$ to the representative x of $\bar{x}$ in the interval $\left(\frac{q}{2}, \frac{q}{2}\right]$ in $\mathbb{Z}$. Clearly, sym_q is not a ring map but it behaves like one whenever the arguments are "sufficiently small". By applying mod_q and sym_q to the coefficients of the polynomials in the bounded polynomial rings $R = \frac{\mathbb{Z}[x]}{(x^N-1)}$ and $R_q = \frac{\mathbb{Z}_q[x]}{(x^N-1)}$, where N is a positive integer, we obtain the maps

$$\mathrm{mod}_q \colon R \to R_q, \qquad \text{and} \qquad \mathrm{sym}_q \colon R_q \to R\,.$$

We will choose many "small" elements from the subset $R\{d,d'\} \subset R$ which consists of those elements of R which have exactly d coefficients equal to 1, d' coefficients equal to -1, and all the remaining coefficients zero. We will see that it is essential for NTRU to work that sym_q behaves like a ring map on certain sums and products of small elements.

Example 3. Let $q > 4$ be a prime power, and $N > 3$. For $(x-1), (x^2 - x) \in R\{1, 1\}$, we have in $\mathbb{Z}[x]$:

$$\begin{aligned}
\mathrm{sym}_q \mathrm{mod}_q\big((x-1)(x^2-x)\big) &= x^3 - 2x^2 + x \\
&= \mathrm{sym}_q \mathrm{mod}_q(x-1) \cdot \mathrm{sym}_q \mathrm{mod}_q(x^2 - x)\,,
\end{aligned}$$

however for $q = 4$, the left hand side evaluates to the polynomial with integral coefficients $x^3 + 2x^2 + x$.

Let us recall quickly,

How and Why NTRU works.

A key in NTRU is made up from two elements, $f \in R\{d_f, d'_f\}$ and $g \in R\{d_g, d'_g\}$, such that the two classes of f in R_3 and in R_q are invertible elements, so there are $f_3^- \in R_3$ and $f_q^- \in R_q$ such that $\mathrm{mod}_3(f) \cdot f_3^- = 1$ and $\mathrm{mod}_q(f) \cdot f_q^- = 1$ hold. The private key is f; the public key is the product $h = 3f_q^- \cdot \mathrm{mod}_q(g)$ in R_q.

Suppose that A wants to send the message $m \in R_3$ to B. For the *encryption*, A chooses a random polynomial r in $R\{d_r, d'_r\}$ and computes

$$e = \mathrm{mod}_q\big(\mathrm{sym}_3(m)\big) + h \cdot \mathrm{mod}_q(r)$$

in R_q, using B's public key h. She sends the encrypted message e to B.

$$\begin{tikzcd}
{} & & {} \arrow[ll, "\mathrm{B}"'] \\
& R \arrow[dl, shift right, "\mathrm{mod}_3"'] \arrow[dr, shift left, "\mathrm{mod}_q"'] & \\
m \in R_3 \arrow[ur, shift right, "\mathrm{sym}_3"'] \arrow[rr, "\mathrm{A}"] & & R_q \ni e \arrow[ul, shift left, "\mathrm{sym}_q"']
\end{tikzcd}$$

The *decryption* of e by B takes place in three steps. First, B eliminates the “big” factor f_q^- of his public key by computing $d_1 = e \cdot \mathrm{mod}_q(f)$ in R_q. We can simplify the right hand side by using that $\mathrm{mod}_q \colon R \to R_q$ is a ring map, and that $f_q^- \cdot \mathrm{mod}_q(f) = 1$.

$$\begin{aligned}
d_1 &= e \cdot \mathrm{mod}_q(f) \\
&= \mathrm{mod}_q\big(\mathrm{sym}_3(m)\big) \cdot \mathrm{mod}_q(f) + h \cdot \mathrm{mod}_q(r) \cdot \mathrm{mod}_q(f) \\
&= \mathrm{mod}_q\big(\mathrm{sym}_3(m) \cdot f\big) + \mathrm{mod}_q(3gr) \cdot f_q^- \cdot \mathrm{mod}_q(f) \\
&= \mathrm{mod}_q\big(\mathrm{sym}_3(m) \cdot f + 3gr\big)\,.
\end{aligned}$$

Next, B computes modulo 3: $d_2 = \mathrm{mod}_3\big(\mathrm{sym}_q(d_1)\big)$. This is the critical step! Indeed, encryption and decryption work only if the element $x = \mathrm{sym}_3(m) \cdot f + 3gr$ computed in the first step is small in the sense that the equality $\mathrm{sym}_q\big(\mathrm{mod}_q(x)\big) = x$ holds, that is that all the coefficients of the polynomial $\mathrm{sym}_3(m) \cdot f + 3gr$ in R are in the interval $\big(\frac{q}{2}, \frac{q}{2}\big]$. Thus, we must have chosen our parameters $d_f, d'_f, d_g, d'_g, d_r, d'_r$ and q in such a way that the equality holds at least with a large probability. If equality holds, we can simplify:

$$\begin{aligned} d_2 &= \mathrm{mod}_3\big(\mathrm{sym}_q(d_1)\big) \\ &= \mathrm{mod}_3\big(\mathrm{sym}_q\big(\mathrm{mod}_q(\mathrm{sym}_3(m) \cdot f + 3gr)\big)\big) \\ &= \mathrm{mod}_3(\mathrm{sym}_3(m) \cdot f + 3gr) \\ &= \mathrm{mod}_3(\mathrm{sym}_3(m) \cdot f) \\ &= m \cdot \mathrm{mod}_3(f)\,. \end{aligned}$$

Finally, we eliminate the factor f by computing in R_3:

$$\begin{aligned} d_3 &= d_2 \cdot f_3^- \\ &= m \cdot \mathrm{mod}_3(f) \cdot f_3^- \\ &= m\,. \end{aligned}$$

3. The checksum problem in NTRU

Each of the rings $R_q = \mathbb{Z}_q[T]/(T^N - 1)$ commonly used in the public key cryptographic system NTRU is a product of at least two factor rings, given by the factorization of $T^N - 1 = (T - 1)(T^{N-1} + T^{N-2} + \cdots + 1)$. Namely, $R_q \cong \mathbb{Z}_q[T]/(T-1) \times \mathbb{Z}_q[T]/(T^{N-1} + \cdots + 1)$, where the first factor is isomorphic to $\mathbb{Z}_q$, and the canonical map $\mathrm{can}_1 : R_q \to \mathbb{Z}_q$ is given by taking the sum of the coefficients of a polynomial representative of an element in R_q, that is, can_1 returns the checksum modulo q.

Our motivation for studying NTRU and for experimenting with our own implementation HERMES of NTRU is the following observation.

Lemma 3.1. *Let q_0 be the greatest common divisor*

$$q_0 = \gcd\{q,\ (d_g - d'_g) \cdot (d_r - d'_r)\}\,,$$

and let for a message $m \in R_3$, c_m be the checksum of $\mathrm{sym}_3(m)$, and $c_e = \mathrm{can}_1(e)$ the checksum modulo q of the encrypted message. Then c_m is congruent to c_e modulo q_0.

In particular, if $d_g = d'_g$ or $d_r = d'_r$ (as in the standard setup for NTRU) then the checksum of the message modulo q is not protected!

Proof. As we are interested in c_m only modulo q, we may replace c_m by $c'_m = \mathrm{can}_1(\mathrm{mod}_q(\mathrm{sym}_3(m)))$. Since can_1 is a ring map we have

$$\begin{aligned}
c_e - c'_m &= \mathrm{can}_1(e - \mathrm{mod}_q \mathrm{sym}_3(m)) \\
&= \mathrm{can}_1(\mathrm{mod}_q(\mathrm{sym}_3(m)) \\
&\qquad + 3f_q^- \mathrm{mod}_q(g) \mathrm{mod}_q(r) - (\mathrm{mod}_q \mathrm{sym}_3(m)) \\
&= \mathrm{can}_1(3f_q^- \mathrm{mod}_q(g) \mathrm{mod}_q(r)) \\
&= \mathrm{can}_1(3) \cdot \mathrm{can}_1(f_q^-) \cdot \mathrm{can}_1(\mathrm{mod}_q(g)) \cdot \mathrm{can}_1(\mathrm{mod}_q(r)) \\
&= \mathrm{can}_1(3) \cdot \mathrm{can}_1(f_q^-) \cdot (d_g - d'_g) \cdot (d_r - d'_r)
\end{aligned}$$

where $\mathrm{can}_1(3)$ and $\mathrm{can}_1(f_q^-)$ are or may be units in $\mathbb{Z}_q$. We obtain from the calculation that q_0 divides $c_e - c'_m$ and hence q_0 divides $c_e - c_m$. $\square$

Remark. I learned on the 33rd International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, 2002) that in commercial implementations of NTRU the checksum problem is avoided by "padding" the message m with extra bits (or rather elements in $\mathbb{Z}_3$).

4. The Internet implementation HERMES

The main advantage of the cryptographic system NTRU is its speed. So even in our implementation HERMES in the (interpreted!) computer language JavaScript, high security levels can be attained when encrypting or decrypting typed text on an internet browser. In this paragraph we describe the role of ring units in the construction of the key, and in the protection of the key and message.

In HERMES we choose N to be one of the numbers 71 (experimental), 191 (average security), 311 (high security), or 479 (very high security). Then the polynomial $T^N - 1$ factors as a product of $T - 1$ and two further non-equivalent irreducible polynomials of the same degree, both over $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

In order to construct polynomials f which have a high probability to be units in $k[T]/(T^N - 1)$, where $k = \mathbb{Z}_q$ or $k = \mathbb{Z}_3$, we use the Corollary after Lemma 1.2. The extra condition that f, when evaluated at $T = 1$, has the value 1, makes sure that the canonical map $\mathrm{can}_1 : k[T]/(T^N - 1) \to k[T]/(T - 1)$ as in Example 1 maps f into a unit. Thus, the probability that a random element f satisfying $f(1) = 1$ is a unit is $\left(1 - \frac{1}{2^{(N-1)/2}}\right)^2$ if $k = \mathbb{Z}_q$ and $\left(1 - \frac{1}{3^{(N-1)/2}}\right)^2$ if $k = \mathbb{Z}_3$. Such elements are in the set $\mathbb{Z}[T]/(T^N - 1)\{d_f, d'_f\}$ whenever $d_f - d'_f = 1$.

There are

$$\frac{N!}{(N-d_f-d'_f)!\, d_f!\, d'_f!}$$

elements in the set $\mathbb{Z}[T]/(T^N-1)\{d_f, d'_f\}$, so the key length of f is given as the base-2 logarithm of this number. Sufficient key lengths have to be chosen

1) for the private key f,

2) for the protection g of f in the public key $h = 3f_q^- g$,

3) for the protection r of the message m in $e = m + hr$, and

4) for the polynomial j computed from a passphrase used to protect the stored version fj^- of the private key. In HERMES we put $d'_f = d_f - 1$ and $d'_j = d_j - 1$ to make it likely that random elements f and j are units; also we put $d'_g = d_g - 1$ and $d'_r = d_r - 1$ to avoid the checksum problem (see Lemma 3.1).

In conclusion, we see that the use of ring units is essential in the operation of the public key cryptographic system NTRU. We consider it important to understand this cryptographic tool well, in particular as it can be implemented, tested, and used in a very flexible setup on the internet.

Acknowledgements. First, I would like to thank my assistant Rita Agrelo for her help in implementing HERMES in the computer language JavaScript. Also, I am grateful for the advice of many of my colleagues, in particular Jim Brewer, Spyros Magliveras, Aaron Meyerowitz, and Ron Mullin.

REFERENCES

[1] ANDERSON, F. W.—FULLER, K. R.: *Rings and Categories of Modules*, Springer Graduate Texts in Mathematics, Vol. 13, Springer-Verlag, Berlin, 1992, p. 376.

[2] BERLEKAMP, E. R.: *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735.

[3] COHN, P. M.: *Algebra Vol. 2*, Second edition, Wiley, p. 428, 1989.

[4] HOFFSTEIN, J.—PIPHER, J.—SILVERMAN, J. H.: *NTRU: A ring based public key cryptosystem*, in: Algorithmic Number Theory (ANTS III), Lect. Notes Comput. Sci., Vol. 1423, Springer-Verlag, Berlin, 1998, pp. 267–288.

Received April 22, 2002

Department of Mathematical Sciences
Florida Atlantic University
Boca Raton, FL 33431
U. S. A.

E-mail: mschmidm@fau.edu