Math 1580 – Problem Set 10. Due Friday Dec. 2, 4pm

Typo corrected 11/30 in Problem 2. Thanks to Keith and Huanzong for the catch.

Problem 1. For each of the following values of N, q and $\mathbf{a}(x)$, either find $\mathbf{a}(x)^{-1}$ in R_q or show that the inverse does not exist.

(a) $N = 5$, $q = 11$, and $\mathbf{a}(x) = x^4 + 8x + 3$.
(b) $N = 5$, $q = 13$, and $\mathbf{a}(x) = x^3 + 2x - 3$.

Problem 2. Let $\mathbf{a}(x) \in (\mathbb{Z}/q\mathbb{Z})[x]$ where q is prime.

(a) Prove that

$$\mathbf{a}(1) \equiv 0 \pmod{q} \quad \text{if and only if} \quad (x-1) \mid \mathbf{a}(x) \quad \text{in } (\mathbb{Z}/q\mathbb{Z})[x]$$

(Hint: polynomial division with remainder works when q is prime.)

(b) Suppose that $\mathbf{a}(1) \equiv 0 \pmod{q}$. Prove that $\mathbf{a}(x)$ is not invertible in R_q. (In particular, ternary polynomials in $\mathcal{T}(d,d) \subset R$ never have inverses in R_q.)

Problem 3. Alice and Bob decide to communicate using the NTRU cryptosystem with parameters $(N, p, q) = (7, 2, 29)$. Alice's public key is

$$\mathbf{h}(x) = 23 + 23x + 23x^2 + 24x^3 + 23x^4 + 24x^5 + 23x^6.$$

Bob sends Alice the plaintext message $\mathbf{m}(x) = 1 + x^5$ using the ephermal key $\mathbf{r}(x) = 1 + x + x^3 + x^6$.

(a) What ciphertext does Bob send to Alice?
(b) Alice's secret key is $\mathbf{f}(x) = 1 + x + x^2 + x^4 + x^5$ and $\mathbf{F}_2(x) = 1 + x^5 + x^6$. Check your answer in (a) by using $\mathbf{f}$ and $\mathbf{F}_2$ to decrypt the message.

Problem 4. The guidelines for choosing NTRU public paramters (N, p, q, d) require that $\gcd(p, q) = 1$. Prove that if $p \mid q$, then it is very easy for Eve to decrypt the message without knowing the private key. (Hint: first do the case $p = q$.)