Summer School – Number Theory for Cryptography, Warwick
Exercises for lectures by D. J. Bernstein and T. Lange, June 27–28, 2013

1. Let $a, b \in \mathbb{F}_{p^n}, c \in \mathbb{F}_p$. Show $(a+b)^p = a^p + b^p$ and $c^p = c$.

2. How quickly can you compute the vector $(f(\alpha), f(-\alpha), f(i\alpha), f(-i\alpha))$ where $i^2 = -1$, given α, i, and $n \geq 1$ coefficients $f_0, f_1, \ldots, f_{n-1}$ of a polynomial $f = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$?

3. How quickly can you compute the vector $(f(\alpha), f(\alpha+1))$ over a field of characteristic 2, given α and $n \geq 1$ coefficients $f_0, f_1, \ldots, f_{n-1}$ of a polynomial $f = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$?

4. Let $E : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6$ be an elliptic curve. Show that the following formulas do in fact describe addition by the chord-and-tangent method.

   Assume that $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$. Then

   $$(x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3),$$

   where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $x_1 \neq x_2$, and $\lambda = (3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1)/(2y_1 + a_1 x_1 + a_3)$ if $(x_1, y_1) = (x_2, y_2)$.

5. Let f, g, m, r be elements of $\mathbf{Z}[x]/(x^p - 1)$ with all coefficients in $\{1, 0, -1\}$.

   (a) How large, in absolute value, can the coefficients of $(1+3f)m + 3rg$ be?

   (b) Assume that r has exactly t coefficients equal to 1 and exactly t coefficients equal to -1. Assume the same of f. How large, in absolute value, can the coefficients of $(1+3f)m + 3rg$ be?

   (c) How large would you *expect* the coefficients to be?

   (d) What if $r = x^i \bar{g}$ and $m = x^j \bar{f}$? Here $\bar{g}$ means the image of g under the ring automorphism $x \mapsto x^{-1}$ ("complex conjugation").

   Context: NTRU decryption works if $(1+3f)m + 3rg$ has coefficients between $-q/2$ and $q/2 - 1$; one can choose q to guarantee that this happens. Standard NTRU parameters are instead chosen so that NTRU decryption *almost always* works. With the original NTRU parameters, there was a noticeable chance of a decryption failure, and these decryption failures were more likely to occur when r and m were correlated with $x^i\bar{g}$ and $x^j\bar{f}$ respectively. Computing the average of $r\bar{r}$ for decryption failures would then reveal $g\bar{g}$, and computing the average of $m\bar{m}$ would then reveal $f\bar{f}$, easily leading to f and g. Oops.

6. Define $\overline{\mathbf{Z}}$ as the ring of algebraic integers in $\mathbf{C}$. Then $\mathbf{Z}[x]$ and $\overline{\mathbf{Z}}[2^{25.5}x]$ are subrings of the polynomial ring $\overline{\mathbf{Z}}[x]$, so their intersection R is also a subring of $\overline{\mathbf{Z}}[x]$.

   (a) Identify generators for the kernel of the ring homomorphism $\sum_i u_i x^i \mapsto \sum_i u_i$ from R to the prime field $\mathbf{Z}/(2^{255} - 19)$.

   (b) Identify a finite subset $S \subseteq R$ that is mapped onto $\mathbf{Z}/(2^{255} - 19)$ by this homomorphism and that, for each i, has at most 2^{30} possible coefficients of x^i.

   (c) Is R a unique-factorization domain?

7. Define $R = \mathbf{Z}/n$, where n is a positive integer. Elements $w = (x, y, z)$ and $w' = (x', y', z')$ of R^3 are called **collinear** if $xy' - x'y = 0$, $xz' - x'z = 0$, and $yz' - y'z = 0$. Show that if w and w' are collinear and $xR + yR + zR + x'R + y'R + z'R = R$ then $Rw + Rw' = Rv$ for some $v \in R^3$. Is this true for all (commutative) rings R?