Math 418/818

Assignment 4

Due 22 October 2015

1. (a) Show that \((\mathbb{Z}/2^r\mathbb{Z})^\times\) is cyclic if and only if \(r \leq 2\).

(b)* Show that \((\mathbb{Z}/p^r\mathbb{Z})^\times\) is always cyclic when \(p\) is an odd prime.

[Hint for part (b)*: Use the results from class to show that \((\mathbb{Z}/p^r\mathbb{Z})^\times\) has an element of order \(p - 1\). Next, show that \(p + 1\) has order \(p^{r-1}\) in \((\mathbb{Z}/p^r\mathbb{Z})^\times\).]

(c) Conclude that \((\mathbb{Z}/m\mathbb{Z})^\times\) is cyclic if and only if \(m = 1, 2, 4, p^r, \text{ or } 2p^r\) for some odd prime \(p\) and some \(r \geq 1\). (You can use the results of (a) and (b).)

2. Let \(G = \langle g \rangle\) be a finite cyclic group of order \(m\), and let \(H \subset G\) be a subgroup of \(G\) of order \(n\). Use results from class to prove that \(n \mid m\) and that \(H = \langle g^{m/n} \rangle\).

3. Let \((a, p) = 1\), where \(p\) is a prime, and let \(n \geq 1\). Prove that the congruence equation \(x^n \equiv a \pmod{p}\) has a solution if and only if \(\text{ord}_p(a) \mid \frac{p-1}{(n, p-1)}\). (Here, \(\text{ord}_p(a)\) denotes the order of \(a\) in \(\mathbb{F}_p^\times\).)

4. Find (by hand) all the primitive roots (generators) in \(\mathbb{F}_{17}^\times\). (Justify your assertions.)

5. Find (by hand) the deciphering function of the affine block cipher

\[f : (\mathbb{Z}/26\mathbb{Z})^3 \rightarrow (\mathbb{Z}/26\mathbb{Z})^3\]

given by \(f(\vec{x}) = A\vec{x} + \vec{b}\) with \(A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 1 & 0 & -1 \end{pmatrix}\) and \(\vec{b} = (1, 2, 3)\). Use this to decipher the encrypted message JYJ (i.e. \((9, 24, 9)\)).

6. MAPLE problem (refer to the MAPLE instruction sheet):

Write a small MAPLE program \(\text{myprimroot}(p)\) which finds the smallest positive integer \(a\) which is a primitive root mod \(p\), where \(p\) is a prime. (Use MAPLE’s order function in the \texttt{numtheory} package.) Test your program for the primes \(p_1 = 48947, p_2 = 48673, p_3 = 104773\) and \(p_4 = 104831\), and compare your result to that obtained by using the function \(\text{primroot}(p)\) in the \texttt{numtheory} package.