UNIVERSITY OF ST ANDREWS

Finite Mathematics Problem Set 3 with solutions

Igor Rivin

December 2, 2015

1 EXERCISE 1

Compute the following cyclotomic polynomials

- $\Phi_1(x)$.
- $\Phi_{17}(x)$
- $\Phi_{1024}(x)$.

Solution:

$$\Phi_1(x) = x - 1, \tag{1.1}$$

$$\Phi_{17}(x) = \sum_{i=0}^{1} 6x^i \tag{1.2}$$

$$\Phi_{1024}(x) = 1 + x^{512} \tag{1.3}$$

2 EXERCISE 2

Show that for all $x > 1$, $(x-1)^{\phi(k)} \leq \Phi_k(x) \leq (x+1)^{\phi(k)}$
Solution: The degree of $Phi_k(x)$ is $\phi(k)$, so it is enough to show that $x - 1 \leq |x - \omega| \leq (x+1)$. That follows from the triangle inequality, since $|\omega| = 1$.

3 EXERCISE 3

We have shown that $GL(2,p)$ has order $(p^2-1)(p^2-p) = p(p-1)(p+1)$. Can you find elements of order $p-1, p, p+1$ in $GL(2,p)$? Solution: The matrix M(a)=$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, for some $a \in F_p^\times$ has order $p-1$ (by Fermat's little theorem). The matrix $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has the property that $B^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, so that has order p. The case $p+1$ is the hardest. Every element of $GF(p^2)$ is the root of a characteristic polynomial of a 2×2 matrix with elements in $GF(p)$. In particular, the multiplicative generator a is such a root, and the matrix $M(a)$ (as above) has order p^2-1. Which means that $M(a)^{p-1}$ has order $p+1$.

4 EXERCISE 4

Draw a picture of the projective plane over a field with 2 elements (meaning, draw its points and lines). Solution: See the picture of the Fano Plane in the Wikipedia article on projective planes: `https://www.wikiwand.com/en/Projective_plane`