Math 418/818

Assignment 3

Due 15 October 2015

1. (a) Use the Chinese Remainder Theorem to find an element of order 12 in $G = (\mathbb{Z}/105\mathbb{Z})^\times$. Are there any elements of larger order in $G$? (Justify your assertions.)

(b)* Use the Chinese Remainder Theorem to find an element of order 10 in $G = (\mathbb{Z}/88\mathbb{Z})^\times$. Are there any elements of larger order in $G$? (Justify your assertions.)

2. Use Fermat’s theorem and Euclid’s Lemma (or CRT) to prove the following.

(a) If $m = pq$ is the product of two distinct primes $p$ and $q$, then for any positive integer $n \equiv 1 \pmod{\phi(m)}$ we have

\[ a^n \equiv a \pmod{m}, \quad \text{for all } a \in \mathbb{Z}. \]

(b)* Prove that (a) is true for all squarefree integers $m > 1$, and give a counterexample to show that it is false when $m$ is not squarefree.

3. (a) Let $G$ be a finite group of order $m$. Prove that $G[n] = G[(n, m)]$, for all $n \geq 1$.

(b) Let $G_1, \ldots, G_r$ be groups, and let $G = G_1 \times \ldots \times G_r$ be the product group. Prove that

\[ G[n] = G_1[n] \times \ldots \times G_r[n], \quad \text{for all } n \geq 1. \]

4. Let $G = (\mathbb{Z}/55\mathbb{Z})^\times$. Use the Chinese remainder theorem and other relevant facts from class (and the problem sets) to find an explicit formula for $t_n := \#G[n]$, for all $n \geq 1$. Evaluate $t_n$ for $n|40$, and use this to calculate the number $N_n$ of elements of order $n$ in $G$, for all $n \geq 1$. (Do not list the elements of $G$.) Is $G$ cyclic?

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

(a) MAPLE’s `numtheory` package contains many useful commands for number theory. (To access these commands, write `with(numtheory):` at the beginning of your MAPLE session.) For example, the command `order(a,m)` computes the order of an integer $a$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. Use this command to find $\text{ord}(123)$ in $(\mathbb{Z}/56323\mathbb{Z})^\times$.

(b) Write a MAPLE program `myord(a,m)` which computes the order of an integer $a$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. (Use a `while` loop and do not use the command `order(.)`.) Test your program and compare your answer for the values of part (a), and also for $a = 12345689$ and $m = 76543211$. 