Number Theory and Group Theory
Exercise Sheet 4

October 31, 2012

1. Let $n$ be a positive integer with prime power decomposition $n = p_1^{a_1} \cdots p_r^{a_r}$. Suppose that $d$ takes the form $p_1^{b_1} \cdots p_r^{b_r}$ with $b_1, \ldots, b_r$ integers satisfying $0 \leq b_i \leq a_i$ for all $i$. Prove that $d$ divides $n$ by exhibiting an integer $e$ such that $de = n$.

2. Prove that there are only finitely many primes of the form $n^2 - 1$ with $n$ an integer. Give a complete list of all such primes.

3. Let $a$ and $b$ be integers with $a = p_1^{a_1} \cdots p_r^{a_r}$ and $b = p_1^{b_1} \cdots p_r^{b_r}$ where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r, b_1, \ldots, b_r$ are non-negative integers. For each $i$ define $m_i = \min\{a_i, b_i\}$ and $M_i = \max\{a_i, b_i\}$.

   (i) Using Proposition 14 of the lecture notes, prove that $(a, b) = p_1^{m_1} \cdots p_r^{m_r}$.

   (ii) Again using Proposition 14, prove that $[a, b] = p_1^{M_1} \cdots p_r^{M_r}$.

   (iii) Establish that for any integers $x$ and $y$ we have the identity $x + y = \min\{x, y\} + \max\{x, y\}$.

   Hence deduce that $(a, b)[a, b] = ab$, or equivalently

   $$[a, b] = \frac{ab}{(a, b)}.$$

---

1Given a finite set of integers $\{a_1, \ldots, a_r\}$ we denote its smallest and largest elements by $\min\{a_1, \ldots, a_r\}$ and $\max\{a_1, \ldots, a_r\}$, respectively.