DLM Assignment 3: Question 4

Simon Stead

January 2015

1 Question 4

Section 3.4 of Joe's report quotes from Lenstra:
"Whether or not kP is defined may depend on the addition chain used (if n is composite)".
It can be proved that if kP is defined for each of two addition chains, then the two outcomes are the same.
Prove this statement for the simplest case, when $N = pq$ with p and q distinct primes.

1.1

Let us define an addition chain as in Joe's report to be $l_t(l_{t-1}(...(l_1P)...)) = kP$ where the l_i are all prime factors of k. Then kP is defined if and only if l_iP is defined for all $1 \leq i \leq t$ if and only if $(l_i, N) = 1$. That is if $l_i \neq p, q$ as $N = pq$ and l_i is prime.
Since we're not considering those points which p,q divide, the set of remaining points on this curve is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{\times}$, and so associativity follows. Therefore

$$l_t(l_{t-1}(...(l_1P)...)) = (l_tl_{t-1}...l_1)P = \sigma(l_tl_{t-1}...l_1)P = \sigma(l_t)(\sigma(l_{t-1})(...(\sigma(l_1)P)...))$$

for some permutation σ of these t objects. This is a different addition chain to the one we started with, so we have kP being defined for two distinct addition chains, producing the same value, as required.