MTH6115 **Cryptography**

Solutions 12

---

1 (a) For every $j \geq 0$, $1 + 2 + 2^2 + 2^3 + \cdots + 2^{j-1} = 2^j - 1 < 2^j$.

(b) Induction. Suppose true for j. So $\sum_{i=1}^{j-1} a_i < a_j$. Add a_j to both sides:

$$\sum_{i=1}^{j} a_i < a_j + a_j \leq a_{j+1}.$$

(c) Easy.

2 The sequence $a_1, \ldots, a_{11}$ is super-increasing, and therefore the unique solution is obtained efficiently using the greedy algorithm, which would also tell us that a solution exists here. We get that $2135 = 1792 + 221 + 108 + 13 + 1$.

3 Clearly this sequence is not super-increasing, even when rearranged into ascending order. The inverse of 1371 modulo 8191 is 6787. Multiplying Bob's public key by 6787 modulo 8191 gives the super-increasing sequence

$$(a'_1, \ldots, a'_{11}) = (1, 5, 12, 26, 54, 113, 230, 466, 939, 1880, 3763).$$

Bob would calculate $b' = 6787 \cdot 11872 \pmod{8191} = 397$ as a subsum of the super-increasing sequence using the greedy algorithm to get that $397 = 54 + 113 + 230$. So, the e_i's are $0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0$ and Alice's message is 00001110000.