Discrete Mathematics MT16: Problem Sheet 4

Chapters 6 (Modular Arithmetic) and 7 (Asymptotic Notation)

4.1 What are the possible values of $x^3 \pmod 7$?

Prove that an integer n cannot be written as the sum of two integer cubes if $n \equiv \pm 3 \pmod 7$. Give a counterexample to show that the converse is false.

4.2 Euclid's Algorithm works because $\gcd(m, n) = \gcd(n - km, m)$ for all $k \in \mathbb{N}$ (though we only use it for $k = n \text{ DIV } m$). Prove this statement.

Hint: Let $\gcd(m, n) = g$*. You need to prove that* $\gcd(n - km, m) = g$*. Use the alternative definition in the lecture notes: it is sufficient to show that i)* $g \mid n - km$*, ii)* $g \mid m$*, and iii)* $l \mid n - km$ *and* $l \mid m$ *together imply* $l \mid g$*.*

4.3 Let $n > 0$ be a fixed modulus. Prove that $m \in \mathbb{Z}_n$ has a multiplicative inverse (i.e. there exists m' satisfying $mm' \equiv 1 \pmod n$) if and only if $\gcd(m, n) = 1$. How many elements of $\mathbb{Z}_{12}$ have a multiplicative inverse (mod 12)?

4.4 Prove that, given any sequence of n integers (not necessarily distinct) $a_1, a_2, \ldots, a_n$, there is some non-empty segment whose elements sum to a multiple of n, i.e. $\sum_{i=l}^{m} a_i \equiv 0 \pmod n$ for some l and m satisfying $1 \leq l \leq m \leq n$.

4.5 Which of the following statements are true? Explain your answers briefly.

(i) $n^{\log_2 3} = O(n^2)$,

(ii) $n + 2n^2 + 3n^3 + 4n^4 = O(n^4)$,

(iii) $\sqrt{n^2 + n \log n} = O(n)$,

(iv) $n^{\log n} = O(n^2)$.

Let $b > 1$ be a constant. For which values of a is it true that $n^a = O(b^n)$? Give a full proof that your answer is correct.

4.6 Consider the recurrence relation.

$$x_0 = 0, \quad x_n = x_{\lfloor \frac{n}{3} \rfloor} + 3x_{\lfloor \frac{n}{5} \rfloor} + n \text{ for } n \geq 1$$

Prove that $x_n = O(n)$.

Hint: show, by strong induction on n*, that* $x_n \leq cn$ *for* $n \geq 0$*, where* c *is a constant you will determine towards the end of the proof.*

4.7 Suppose that $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$. Prove that $f_1(n)f_2(n) = O(g_1(n)g_2(n))$.

Is it true that, under the same conditions, $f_1(n)/f_2(n) = O(g_1(n)/g_2(n))$?