Discrete Mathematics (Sheet #4)

Marius Gavrilescu

1. $\{0, 1, 6\}$ are the possible values of $x^3 \pmod 7$. The possible values modulo 7 of a sum of two integer cubes are $\{a + b \pmod 7 | a, b \in \{0, 1, 6\}\} = \{0, 1, 2, 5, 6\}$. Therefore a number $n \equiv \pm 3 \pmod 7$ cannot be written as a sum of two integer cubes.

   Counterexample: 5 cannot be written as a sum of two integer cubes, yet $5 \not\equiv \pm 3 \pmod 7$.

2. Suppose $d | \gcd(m, n) \implies d|m \wedge d|n \implies d|m \wedge d|km \wedge d|n \forall k \in \mathbb{N} \implies d|m \wedge d|n - km \forall k \in \mathbb{N} \implies d | \gcd(n - km, m)$.

   Suppose $d | \gcd(n-km, m) \implies d|n-km \wedge d|m \implies d|n-km \wedge d|km \wedge d|m \implies d|n \wedge d|m \implies d | \gcd(n, m)$.

   So the left hand side and the right hand side have the same divisors, hence they are equal.

3. If $\gcd(m, n) = d > 1$ then any number mm' will be a multiple of d, and $mm' \equiv kd \neq 1 \pmod n$. So m does not have a multiplicative inverse.

   Now suppose $\gcd(m, n) = 1$ and suppose m does not have a multiplicative inverse. Take the numbers $A = \{m, 2m, \ldots, nm\}$. There are n numbers and $n-1$ possible residues modulo n (1 is not possible). By the pigeonhole principle there must exist $k \neq k'$ such that $km \equiv k'm \pmod n$. But then $n|(|k - k'|)m$. As $\gcd(n, m) = 1$, we get $n|k - k'$, and since $1 \leq k, k' \leq n$ we get $k = k'$, contradiction.

   Four elements of $\mathbb{Z}_{12}$ have a multiplicative inverse: $1, 5, 7, 11$.

4. Take the n sums $s_k = \sum_{i=1}^{k}, 1 \leq k \leq n$. If one of this sums is a multiple of n, the problem is finished. Otherwise we have n sums and $n - 1$ possible residues modulo n (0 is not possible). Therefore there exist $a < b$ such that $s_a \equiv s_b \pmod n$. But then $n|s_b - s_a = \sum_{i=a+1}^{b}$, so we found one such sum.

5. (a) True, since $n^{\log_2 3} \leq n^2$ for $n \geq 1$.

   (b) True, since $n + 2n^2 + 3n^3 + 4n^4 \leq n^4 + 2n^4 + 3n^4 + 4n^4 = 10n^4$ for $n \geq 1$.

   (c) True, since $\sqrt{n^2 + n \log n} \leq \sqrt{n^2 + n^2} = \sqrt{2}n$ for $n \geq 1$.

   (d) False, since $\frac{n^{\log n}}{n^2} = n^{\log n - 2}$ which is unbounded.

   $\log \frac{n^a}{b^n} = \log n^a - \log b^n = a \log n - n \log b$.

   $(a \log n - n \log b)' = \frac{a}{n} - \log b$, which is negative for sufficiently large n, so $a \log n - n \log b$ is bounded, so $\log \frac{n^a}{b^n}$ is bounded, so $n^a = O(b^n)$ for all values of a.

6. Base case: $0 = x_0 \leq 15 \cdot 0$.

   Suppose $x_k \leq 15k \forall k < n$. Then $x_n = x_{\lfloor \frac{n}{3} \rfloor} + 3x_{\lfloor \frac{n}{5} \rfloor} + n \leq 15\lfloor \frac{n}{3} \rfloor + 3 \cdot 15 \lfloor \frac{n}{5} \rfloor + n \leq 5n + 9n + n = 15n$.

   So $x_n = O(n)$.

7. We have $|f_1(n)| < c_1|g_1(n)| \forall n \geq N_1$ and $|f_2(n)| < c_2|g_2(n)| \forall n \geq N_2$. Therefore $|f_1(n)||g_1(n)| < c_1c_2|g_1(n)||g_2(n)| \forall n > \max(N_1, N_2) \implies |f_1(n)f_2(n)| < (c_1c_2)|g_1(n)g_2(n)| \forall n \geq \max(N_1, N_2)$. So $f_1(n)f_2(n) = O(g_1(n)g_2(n))$.

   The second part is false. Counterexample: $f_1 = g_1 = g_2 = \mathrm{id}, f_2(n) = \frac{1}{n}$. Left hand side is linear, right hand side is constant.