DMMR Tutorial sheet 5

Number theory

October 21, 2015

Some of the exercises for this tutorial are taken the book: Kenneth Rosen, Discrete Mathematics and its Applications, 7th Edition, McGraw-Hill, 2012.

1. Analogous to the definition of $\gcd$ we define the least common multiple (lcm) in the following way:
   For two numbers a and b with the prime factorisation $a = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$, $b = p_1^{b_1} \cdot \ldots \cdot p_n^{b_n}$ we define
   $$\text{lcm}(a, b) := p_1^{\max(a_1, b_1)} \cdot \ldots \cdot p_n^{\max(a_n, b_n)}$$
   Show that if a and b are positive integers, then $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.
2. Show that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$
3. Use the Euclidean Algorithm to find
   (a) $\gcd(12, 18)$
   (b) $\gcd(111, 201)$
   (c) $\gcd(1001, 1331)$
   (d) $\gcd(12345, 54321)$
   (e) $\gcd(1000, 5040)$
   (f) $\gcd(9888, 6060)$
4. Prove that the product of any three consecutive integers is divisible by 6
5. This question uses Fermat's little theorem.
   (a) Use Fermat's little theorem to compute $3^{302} \bmod 11$ and $3^{302} \bmod 13$
   (b) Show with the help of Fermat's little theorem that if n is a positive integer, then 42 divides $n^7 - n$.

Solutions (to the last question on the sheet) must be handed in on paper at the ITO by Wednesday, 28 October, 4:00pm. Please post it into the grey metal box on the wall outside the ITO.