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 $a = p_1^{a_1} \cdots p_n^{a_n}$, $b = p_1^{b_1} \cdots p_n^{b_n}$ we define
   
   $$\text{lcm}(a, b) := p_1^{\max(a_1, b_1)} \cdots p_n^{\max(a_n, b_n)}$$

   Show that if $a$ and $b$ are positive integers, then $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

   **Solution:**
   
   Take a set of primes $\{p_1, p_2, \ldots, p_n\}$ and natural numbers $\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$ such that $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$. Then,
   
   $$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$
   $$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

   Thus,
   
   $$\gcd(a, b) \cdot \text{lcm}(a, b) = p_1^{\min(a_1, b_1)} p_1^{\max(a_1, b_1)} p_2^{\min(a_2, b_2)} p_2^{\max(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)} p_n^{\max(a_n, b_n)}$$
   $$= p_1^{\min(a_1, b_1) + \max(a_1, b_1)} p_2^{\min(a_2, b_2) + \max(a_2, b_2)} \cdots p_n^{\min(a_n, b_n) + \max(a_n, b_n)}$$

   Moreover, for every $x, y$ it is true that $\min(x, y) + \max(x, y) = x + y$. Therefore,
   
   $$\gcd(a, b) \cdot \text{lcm}(a, b) = p_1^{a_1 + b_1} p_2^{a_2 + b_2} \cdots p_n^{a_n + b_n}$$
   $$= p_1^{a_1} p_1^{b_1} p_2^{a_2} p_2^{b_2} \cdots p_n^{a_n} p_n^{b_n}$$
   $$= ab$$

2. 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) $\gcd(9888, 6060)$

   **Solution:**
3. This question uses Fermat’s little theorem.

(a) Use Fermat’s little theorem to compute $3^{304} \mod 11$ and $3^{304} \mod 13$

Solution:

(a) Fermat’s little theorem tells us that $3^{10} \equiv 1 \pmod{11}$. Then, $3^{300} \equiv (3^{10})^{30} \equiv 1^{30} \equiv 1 \pmod{11}$. Therefore, $3^{304} \mod 11 = 4$.

Similarly, $3^{12} \equiv 1 \pmod{13}$. Then, $3^{300} \equiv (3^{12})^{25} \equiv 1^{25} \equiv 1 \pmod{13}$. Therefore, $3^{304} \mod 13 = 3$.

(b) To show 42 divides $n^7 - n$, we show $2 \times 3 \times 7$ divides $n^7 - n$. So, we prove $n^7 - n$ is divisible by 2, 3 and 7 respectively.

Case 1, we prove 2 divides $n^7 - n$. There are two cases. If n is even, 2 divides $n^7 - n$. If n is odd, we have $n^7 - n = n(n^6 - 1)$ and $n^6 - 1$ is even since $n^6$ is odd. Therefore, 2 divides $n(n^6 - 1)$.

Case 2 we prove 3 divides $n^7 - n$. If 3 divides $n^7 - n$, it is done. If not then 3 doesn’t divide n as it is a factor of $n^7 - n$. So by Fermat’s little theorem, we know $n^{3-1} \equiv 1 \pmod{3}$ since 3 and n are coprime. Then $(n^2)^3 \equiv (1)^3 = 1 \pmod{3}$. So therefore 3 divides $n^6 - 1$ and so 3 divides $n^7 - n$.

Case 3 prove 7 divides $n^7 - n$. If 7 divides $n^7 - n$, it is done. If not then 7 doesn’t divide n as it is a factor of $n^7 - n$. Therefore, by Fermat’s little theorem, we know $n^{7-1} \equiv 1 \pmod{7}$ since 7 and n are coprime. Then 7 divides $n^6 - 1$ and so 7 divides $n^7 - n$.


4. (a) Find the least integer n such that $f(x)$ is $O(x^n)$ for each of these functions.

i. $f(x) = 2x^3 + x^2 \log x$

ii. $f(x) = 3x^3 + (\log x)^4$

iii. $f(x) = (x^4 + x^2 + 1)/(x^3 + 1)$

Solution:

i. It is clear that n is at least 3. Moreover, 2 is $O(1)$ and $\log x$ is $O(x)$. Thus, the multiplications $2x^3$ and $x^2 \log x$ are $O(1 \cdot x^3) = O(x^2 \cdot x) = O(x^3)$. Then, the sum $2x^3 + x^2 \log x$ is also $O(x^3)$. Therefore, $n = 3$. 


ii. It is clear that $n$ is at least 3 and $3x^3$ is $O(x^3)$. Moreover, $(\log x)^4$ is $O(x)$. Thus, the sum $3x^3 + (\log x)^4$ is $O(x^3)$. Therefore, $n = 3$.

iii. We rewrite the expression as $x^4/(x^3 + 1) + (x^2 + 1)/(x^3 + 1)$. It is clear that $(x^2 + 1)/(x^3 + 1)$ is $O(1)$. Moreover, for $x > 0$ we have that $x^4/(x^3 + 1) < x$ and thus $x^4/(x^3 + 1)$ is $O(x)$. Thus, $x^4/(x^3 + 1) + (x^2 + 1)/(x^3 + 1)$ is $O(x)$. To prove that it is not $O(1)$, we show that for any positive constant $c$, if $x > c + 1$ then $x^4/(x^3 + 1) > c$. This is true because for any $c$ positive $(c + 1)^4 = c(c + 1)^3 + (c + 1) > c(c + 1)^3 + c = c((c + 1)^3 + 1)$. Thus, $(c + 1)^4/((c + 1)^3 + 1) > c$. Thus, we have shown that $x^4/(x^3 + 1)$ exceeds any constant at some point and thus $x^4/(x^3 + 1)$ is not $O(1)$. From this we can conclude that $n = 1$.

\[\square\]

(b) Let $f_1(x)$ and $f_2(x)$ be functions from the set of real numbers to the set of positive real numbers. Show that if $f_1(x)$ and $f_2(x)$ are both $\Theta(g(x))$, where $g(x)$ is a function from the set of real numbers to the set of positive real numbers, then $f_1(x) + f_2(x)$ is $\Theta(g(x))$. Is this still true if $f_1(x)$ and $f_2(x)$ can take negative values?

**Solution:**

Let $l_1, u_1, k_1$ and $l_2, u_2, k_2$ be witnesses that $f_1(x)$ and $f_2(x)$ are $\Theta(g(x))$, respectively. Let $l = l_1 + l_2$, $u = u_1 + u_2$ and $k = \max(k_1, k_2)$. Then, for $x > k$ we have that $l_1|g(x)| < |f_1(x)| < u_1|g(x)|$ and $l_2|g(x)| < |f_2(x)| < u_2|g(x)|$. If we sum both inequalities we get that for all $x > k$ we have that $l|g(x)| = (l_1 + l_2)|g(x)| = l_1|g(x)| + l_2|g(x)| < |f_1(x)| + |f_2(x)| < u_1|g(x)| + u_2|g(x)| = (u_1 + u_2)|g(x)| = u|g(x)|$. Using the fact that $f_1(x)$ and $f_2(x)$ only take positive values we can see that $|f_1(x) + f_2(x)| = |f_1(x) + f_2(x)|$. Thus, $l$, $u$ and $k$ are witnesses that $f_1(x) + f_2(x)$ is $\Theta(g(x))$.

Take $g(x) = f_1(x) = x$ and $f_2(x) = -x$ to show that if the functions can take negative values then the result is not true. It is trivial to check that $f_1(x)$ and $f_2(x)$ are both $\Theta(g(x))$. However, $f_1(x) + f_2(x) = 0$, which is not $\Theta(g(x))$ because for any $l$, $l|g(x)|$ exceeds 0 for every $x \neq 0$.

\[\square\]

5. Using the Chinese Remainder Theorem, find a solution to the following system of equivalences.

\[
\begin{align*}
x &\equiv 1 \pmod{2} \\
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 4 \pmod{11}
\end{align*}
\]

Explain your calculations.

**Solution:**

By the Chinese Remainder Theorem we know the solution is

\[
(a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4) \mod m
\]

where $m = (2 \times 3 \times 5 \times 11) = 330$; $a_1 = 1$, $M_1 = m/2 = 165$ and $y_1 = 1$ is the inverse of $M_1$ mod 2 (that is, the unique $y_1$ mod 2 such that $y_1 \times M_1 \equiv 1 \pmod{2}$); $a_2 = 2$, $M_2 = m/3 = 110$ and $y_2 = 2$ is the inverse of $M_2$ mod 3; $a_3 = 3$, $M_3 = m/5 = 66$ and $y_3 = 1$; $a_4 = 4$, $M_4 = m/11 = 30$ and $y_4 = 7$.

So the solution is $165 + 440 + 198 + 840 \mod 330 = 323$.

(For full marks, the answer should identify the calculations of $m$, the $M_i$ and the inverses $y_i$, $1 \leq i \leq 4$.)

\[\square\]
Solutions (to the last question on the sheet) must be handed in on paper at the ITO by Wednesday, 26 October, 4:00pm. Please post it into the grey metal box on the wall outside the ITO.