DMMR Tutorial sheet 5

Number theory

October 17th, 2019

1. Analogous to the definition of $\gcd$ we define the least common multiple (lcm) in the following way: for two positive integers a and b with the prime factorisation $a = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$, $b = p_1^{b_1} \cdot \ldots \cdot p_n^{b_n}$ let
$$\text{lcm}(a, b) := p_1^{\max(a_1,b_1)} \cdot \ldots \cdot p_n^{\max(a_n,b_n)}$$
Show that if a and b are positive integers, then $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

2. Use the Euclidean algorithm to find
   (a) $\gcd(18, 12)$
   (b) $\gcd(201, 111)$
   (c) $\gcd(1331, 1001)$
   (d) $\gcd(54321, 12345)$
   (e) $\gcd(5040, 1000)$
   (f) $\gcd(9888, 6060)$

3. Recall in lectures we introduced the extended Euclidean algorithm below to compute for positive x, y not only $d = \gcd(x, y)$ but also the Bézout coefficients (the integers a and b such that $d = ax + by$). The relation x div y is the quotient, the q such that $x = yq + r$ where $0 \leq r < y$ is the remainder x mod y (from the division algorithm).
```
algorithm e-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d,a,b) := e-gcd(y,x mod y)
     return((d,b,a - ((x div y) * b)))
```
Compute the triples (d, a, b) for the following x and y.
   (a) $x = 18, y = 12$
   (b) $x = 201, y = 111$
   (c) $x = 1331, y = 1001$

4. This question uses Fermat's little theorem.
   (a) Use Fermat's little theorem to compute 3^{304} mod 11 and 3^{304} mod 13
   (b) Show with the help of Fermat's little theorem that if n is a positive integer, then 42 divides $n^7 - n$.

5. (a) Let a, b, c, d, m be integers. Find counter examples to each of the following statements about congruences:

   i. if $ac \equiv bc \pmod{m}$ with $m \geq 2$, then $a \equiv b \pmod{m}$

   ii. if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$

   (b) Using the Chinese Remainder Theorem, find a solution to the following system of equivalences.

$$
\begin{aligned}
x &\equiv 1 \pmod{2} \\
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 4 \pmod{11}
\end{aligned}
$$

   Explain your calculations.