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 $ab = \gcd(a,b) \cdot \text{lcm}(a,b)$.

   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,

   $$\begin{aligned}\gcd(a,b) &= p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)} \\ \text{lcm}(a,b) &= p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}\end{aligned}$$

   Thus,

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

   Moreover, for every x, y it is true that $\min(x,y) + \max(x,y) = x + y$. Therefore,

   $$\begin{aligned}\gcd(a,b) \cdot \text{lcm}(a,b) &= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n} \\ &= p_1^{a_1} p_1^{b_1} p_2^{a_2} p_2^{b_2} \cdots p_n^{a_n} p_n^{b_n} \\ &= ab\end{aligned}$$

   $\square$

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 $a \equiv b \pmod{n}$

   Solution:
   The hypothesis $a \equiv b \pmod{m}$ means that $a = b + k_1 \cdot m$ for some $k_1 \in \mathbb{N}$. $m \mid (a - b)$. Since we are given that $n \mid m$, see Lecture 10 slides, this implies that $n \mid (a - b)$. By definition therefore $a \equiv b \pmod{n}$. $\square$

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) $\gcd(9888, 6060)$

Solution:

(a) $\gcd(12, 18) = \gcd(12, 6) = \gcd(6, 0) = 6$
(b) $\gcd(111, 201) = \gcd(111, 90) = \gcd(90, 21) = \gcd(21, 6) = \gcd(6, 3) = \gcd(3, 0) = 3$
(c) $\gcd(1001, 1331) = \gcd(1001, 330) = \gcd(330, 11) = \gcd(11, 0) = 11$
(d) $\gcd(12345, 54321) = \gcd(12345, 4941) = \gcd(4941, 2463) = \gcd(2463, 15) = \gcd(15, 3) = \gcd(3, 0) = 3$
(e) $\gcd(1000, 5040) = \gcd(1000, 40) = \gcd(40, 0) = 40$
(f) $\gcd(9888, 6060) = \gcd(6060, 3828) = \gcd(3828, 2232) = \gcd(2232, 1596) = \gcd(1596, 636) = \gcd(636, 324) = \gcd(324, 312) = \gcd(312, 12) = \gcd(12, 0) = 12$

$\square$

4. Prove that the product of any three consecutive integers is divisible by 6

Solution:
We first prove the smaller version:
Every product of two consecutive integers is divisible by 2. The product can be written as $a(a+1)$. Consider the two following cases for a.

- If a is even, we can write $a = 2k$ for some $k \in \mathbb{Z}$. With this we get $a(a+1) = 2k(2k+1) = 2(2k^2 + k)$. Since $2k^2 + k \in \mathbb{Z}$ this is divisible by 2.
- If a is odd, then we can write $a = 2k + 1$ for some $k \in \mathbb{Z}$. With this we get $a(a + 1) = (2k + 1)(2k + 2) = 2(2k^2 + 3k + 1)$. Since $2k^2 + 3k + 1 \in \mathbb{Z}$, this is divisible by 2.

The same proof can be carried out for "$a(a + 1)(a + 2)$ is divisible by 3" in 3 cases.

With these two lemmas we can prove the desired statement: We showed the proof that $a(a + 1)(a + 2)$ is divisible by 3. Since $a(a + 1) \mid a(a + 1)(a + 2)$ and $2 \mid a(a + 1)$ we get that $2|a(a + 1)(a + 2)$. Combining these two we get $2 * 3 = 6|a(a + 1)(a + 2)$.

The general statement we used during this proof is "$\prod\limits_{i=0}^{n-1} a + i$ is divisible by n". We extend our proof to this statement: Consider $k = a \bmod n$. This value is per definition in $\{0, ..., n - 1\}$.

- If $k = 0$, then $a = m \cdot n$ for some $m \in \mathbb{N}$. And we get

$$\prod_{i=0}^{n-1} (a + i) = n \cdot \left(m \cdot \prod_{i=1}^{n-1} (a + i) \right)$$

  with $\left(m \cdot \prod\limits_{i=1}^{n-1} (a + i) \right) \in \mathbb{Z}$, which means the product is divisible by n.

- If $k \in \{1, ..., n-1\}$ we get that $l = n - k \in \{1, ..., n-1\}$. Then we can write the product as
$$\prod_{i=0}^{l-1}(a+i) \cdot (a+l) \cdot \prod_{i=l+1}^{n-1}(a+i)$$
Furthermore we know from the definition of mod that $a = m \cdot n + k$ for some $m \in \mathbb{Z}$. This means $a + l = m \cdot n + k + (n-k) = (m+1) \cdot n$ and we get
$$\prod_{i=0}^{n-1}(a+i) = n \cdot \left((m+1) \cdot \prod_{i=1}^{l-1}(a+i) \cdot \prod_{i=l+1}^{n-1}(a+i)\right)$$
with $\left((m+1) \cdot \prod_{i=1}^{l-1}(a+i) \cdot \prod_{i=l+1}^{n-1}(a+i)\right) \in \mathbb{Z}$, which means the product is divisible by n.

$\square$

5. This question uses Fermat's little theorem.

   (a) Use Fermat's little theorem to compute 3^{302} mod 11 and 3^{302} mod 13

   (b) Show with the help of Fermat's little theorem that if n is a positive integer, then 42 divides $n^7 - n$.

   Solution:

   (a) (4 marks) Fermat's little theorem tells us that $3^{10} \equiv 1 \bmod 11$. Then, $3^{300} \equiv (3^{10})^{30} \equiv 1^{30} \equiv 1 \bmod 11$. Thus, $3^{302} = 3^2 \cdot 3^{300} \equiv 3^2 \cdot 1 \equiv 9 \bmod 11$. Therefore, $3^{302} \bmod 11 = 9$. Similarly, $3^{12} \equiv 1 \bmod 13$. Then, $3^{300} \equiv (3^{12})^{25} \equiv 1^{25} \equiv 1 \bmod 13$. Thus, $3^{302} = 3^2 \cdot 3^{300} \equiv 3^2 \cdot 1 \equiv 9 \bmod 13$. Therefore, $3^{302} \bmod 13 = 9$.

   (b) (7 marks) To show 42 divides $n^7 - n$, it is to show $2 \times 3 \times 7$ divides $n^7 - n$. We can prove $n^7 - n$ is divisible by 2, 3 and 7 respectively.
   Case 1, 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. Then 2 divides $n(n^6 - 1)$.
   Case 2 prove 3 divides $n^7 - n$. If 3 divides $n^7 - n$, it is done. If not, by Fermat's little theorem, we know $n^{3-1} \equiv 1 \bmod 3$ since 3 and n are coprime. Then $(n^2)^3 \equiv (1)^3 = 1$. Then 3 divides $n^6 - 1$. Then 3 divides $n^7 - n$.
   Case 3 prove 7 divides $n^7 - n$. If 7 divides $n^7 - n$, it is done. If not, by Fermat's little theorem, we know $n^{7-1} \equiv 1 \bmod 7$ since 7 and n are coprime. Then 7 divides $n^6 - 1$. Then 7 divides $n^7 - n$.

$\square$

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.