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

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. 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) $\gcd(9888, 6060)$

Solution:

   (a) $\gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$

(b) $\gcd(201, 111) = \gcd(111, 90) = \gcd(90, 21) = \gcd(21, 6) = \gcd(6, 3) = \gcd(3, 0) = 3$

(c) $\gcd(1331, 1001) = \gcd(1001, 330) = \gcd(330, 11) = \gcd(11, 0) = 11$

(d) $\gcd(54321, 12345) = \gcd(12345, 4941) = \gcd(4941, 2463) = \gcd(2463, 15) = \gcd(15, 3) = \gcd(3, 0) = 3$

(e) $\gcd(5040, 1000) = \gcd(1000, 40) = \gcd(40, 0) = 40$

(f) $\gcd(9888, 6060) = \gcd(6060, 3828) = \gcd(3828, 2232) = \gcd(2232, 1596) = \gcd(1596, 636) = \gcd(636, 324) = \gcd(324, 312) = \gcd(312, 12) = \gcd(12, 0) = 12$

□

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) $x = 1331, y = 1001$

Solution:
That the algorithm is correct for computing Bézout coefficients follows from observations (discussed in lectures) which includes the following: assume $x = yq + r$ via division algorithm where $r = x \bmod y$ and $q = x \operatorname{div} y$ and assume $d = ay + br$; so, $r = x - yq$ and, therefore, $d = ay + b(x - yq) = bx + (a - qb)y$, as required.

(a) We do the calls to e-gcd in reverse, so the returns are in order.

$$\begin{aligned}
\text{e-gcd}(6, 0) &= (6, 1, 0).\ \text{So } 6 = 1 * 6 + 0 * 0 \\
\text{e-gcd}(12, 6) &= (6, 0, 1 - (2 * 0)) = (6, 0, 1).\ \text{So } 6 = 0 * 12 + 1 * 6 \\
\text{e-gcd}(18, 12) &= (6, 1, 0 - (1 * 1)) = (6, 1, -1).\ \text{So } 6 = 1 * 18 + -1 * 12
\end{aligned}$$

$6 = 1 * 18 + -1 * 12$

(b)

$$\begin{aligned}
\text{e-gcd}(3, 0) &= (3, 1, 0).\ \text{So } 3 = 1 * 3 + 0 * 0 \\
\text{e-gcd}(6, 3) &= (3, 0, 1 - (2 * 0)) = (3, 0, 1).\ \text{So } 3 = 0 * 6 + 1 * 3 \\
\text{e-gcd}(21, 6) &= (3, 1, 0 - (3 * 1)) = (3, 1, -3).\ \text{So } 3 = 1 * 21 + -3 * 6 \\
\text{e-gcd}(90, 21) &= (3, -3, 1 - (4 * -3)) = (3, -3, 13).\ \text{So } 3 = -3 * 90 + 13 * 21 \\
\text{e-gcd}(111, 90) &= (3, 13, -3 - (1 * 13)) = (3, 13, -16).\ \text{So } 3 = 13 * 111 + -16 * 90 \\
\text{e-gcd}(201, 111) &= (3, -16, 13 - (1 * -16)) = (3, -16, 29).\ \text{So } 3 = -16 * 201 + 29 * 111
\end{aligned}$$

$3 = -16 * 201 + 29 * 111 = -3216 + 3219$

(c)

$$\begin{array}{lcl}
\text{e-gcd}(11,0) & = & (11,1,0).\ \text{So } 11 = 1*11+0*0 \\
\text{e-gcd}(330,11) & = & (11,0,1-(30*0)) = (11,0,1).\ \text{So } 11 = 0*330+1*11 \\
\text{e-gcd}(1001,330) & = & (11,1,0-(3*1)) = (11,1,-3).\ \text{So } 11 = 1*1001+-3*330 \\
\text{e-gcd}(1331,1001) & = & (11,-3,1-(1*-3)) = (11,-3,4).\ \text{So } 11 = -3*1331+4*1001
\end{array}$$

$11 = -3*1331+4*1001 = -3993+4004$

□

4. This question uses Fermat's little theorem.

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

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

   Solution:

   (a) Fermat's little theorem tells us that $3^{10} \equiv 1 \pmod{11}$. Then, $3^{300} \equiv (3^{10})^{30} \equiv 1^{30} \equiv 1 \pmod{11}$. Thus, $3^{304} = 3^4 \cdot 3^{300} \equiv 3^4 \cdot 1 \equiv 4 \pmod{11}$. Therefore, $3^{304} \bmod 11 = 4$.
   Similarly, $3^{12} \equiv 1 \pmod{13}$. Then, $3^{300} \equiv (3^{12})^{25} \equiv 1^{25} \equiv 1 \pmod{13}$. Thus, $3^{304} = 3^4 \cdot 3^{300} \equiv 3^4 \cdot 1 \equiv 3 \pmod{13}$. Therefore, $3^{304} \bmod 13 = 3$.

   (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 $n^7 - n$.

□

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 $a^c \equiv b^d \pmod m$

   Solution:

      i. With $m = c = 2$ and $a = 0, b = 1$ we get $ac \equiv 0 \cdot 2 \equiv 0 \equiv 2 \equiv 1 \cdot 2 \equiv bc \pmod 2$, but $0 \bmod 2 = 0 \neq 1 = 1 \bmod 2$ and therefore $0 \not\equiv 1 \pmod 2$

      ii. With $m = 3$, $a = 2 \equiv 5 = b \pmod 3$ and $c = 4 \equiv 1 = d \pmod 3$ we get $a^c \bmod 3 = 2^4 \bmod 3 = 16 \bmod 3 = 1$, but $b^d \bmod 3 = 5^1 \bmod 3 = 5 \bmod 3 = 2$. Since $1 \neq 2$ it follows that $a^c \not\equiv b^d \pmod m$

$\square$

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

$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 4 \pmod{11}$$

Explain your calculations.

Solution:

By the Chinese Remainder Theorem we know the solution is

$$(a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4) \bmod m$$

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 $165 + 440 + 198 + 840 \pmod{330} \equiv 323 \pmod{330}$. $\square$