Homework 4

Suyi Liu

March 7, 2017

1 Problem 1

The algorithm:
Compute gcd(m,n) first and then get x = m/gcd(m,n), and y = n/gcd(m,n). Then lcm(m,n) = gcd(m,n)*x*y.

Proof:
Suppose a = $p_1^{a_1} * p_2^{a_2} * ... * p_n^{a_n}$, b = $p_1^{b_1} * p_2^{b_2} * ... * p_n^{b_n}$, since gcd(m,n) gives us $p_1^{Min(a_1,b_1)} * p_2^{Min(a_2,b_2)} * ... * p_n^{Min(a_n,b_n)}$, gcd(m,n)*x*y = $p_1^{Max(a_1,b_1)} * p_2^{Max(a_2,b_2)} * ... * p_n^{Min(a_n,b_n)}$.
Because, x = $m/gcd(m,n) = \prod_{i=1}^{n}(p_i^{a_n-b_n}$ if $a_n > b_n$, or p_i^0 otherwise), and y = $n/gcd(m,n) = \prod_{i=1}^{n}(p_i^{b_n-a_n}$ if $b_n > a_n$, or p_i^0 otherwise). So gcd(m,n)*x*y = $\prod_{i=1}^{n}(p_i^{b_n+a_n-b_n}$ if $a_n \geq b_n$, or $p_i^{a_n+b_n-a_n}$ if $b_n > a_n$) So gcd(m,n)*x*y = $p_1^{Max(a_1,b_1)} * p_2^{Max(a_2,b_2)} * ... * p_n^{Max(a_n,b_n)}$.

Now prove prove gcd(m,n)*x*y is lcm(m,n): Since x = m/gcd(m,n), m = gcd(m,n)*x, so m|gcd(m,n)*x*y. And similarly, y = n/gcd(m,n), n = gcd(m,n)*y, so n|gcd(m,n)*x*y.
Now prove there's no common multiple that is smaller than gcd(m,n)*x*y. Since m = gcd(m,n)*x, gcd(m,n)*x*y = m*y. Since common multiple must be a multiple of m, let's suppose the smallest common multiple is m*y', and $y' < y$. Since y = $n/gcd(m,n) = \prod_{i=1}^{n}(p_i^{b_n-a_n}$ if $b_n > a_n$, or p_i^0 otherwise), let's suppose $y' = y$, except for some p_i, the term equals $p_i^{b_n-a_n-c}$ when $b_n > a_n$. So in this case m*y' = $\prod_{i=1}^{n}(p_i^{a_n}$ if $a_n \geq b_n$, or $p_i^{a_n+b_n-a_n}$ if $b_n > a_n$), except for some p_i the term equals $p_i^{b_n-c}$ if $b_n > a_n$). However, in this case, n will not divide m*y because n has $p_i^{b_n}$ as a factor. Which leads to contradiction. So gcd(m,n)*x*y must be the smallest least common multiple of m and n.

2 Problem 2

Suppose $c^{\frac{1}{d}}$ is rational. It cam be expressed by $\frac{m}{n}$, where m and n are relatively prime. If m and n are not relatively prime, we divide them both by gcd(m,n) to get a numerator and a denominator that are relatively prime to each other.

So there is no common factor between m and n.

Then $(c^{\frac{1}{d}})^d = c = \frac{m^d}{n^d}$. Suppose $m = p_u^{a_u} * p_v^{a_v} * ... * p_w^{a_w}$, and $n = p_r^{a_r} * p_s^{a_s} * ... * p_t^{a_t}$, then $m^d = p_u^{d*a_u} * p_v^{d*a_v} * ... * p_w^{d*a_w}$, and $n^d = p_r^{d*a_r} * p_s^{d*a_s} * ... * p_t^{d*a_t}$, Since m^d and n^d are still relatively prime(no common prime factors), $\frac{m^d}{n^d}$ is not an integer, which contradicts the premise that c is an integer. So if $c^{\frac{1}{d}}$ is not an integer, it is irrational.

3 Problem 3

Suppose the given fraction is $\frac{b}{a}$. Since according to Division Lemma, $a = qb + r$, where q and r are unique integers. Then $\frac{b}{a} = \frac{b}{qb+r} = \frac{1}{\frac{qb+r}{b}} = \frac{1}{q+\frac{r}{b}}$. And in the same way $\frac{r}{b}$ can be written as $\frac{r}{q_2 r + r_2} = \frac{1}{\frac{q_2 r + r_2}{r}} = \frac{1}{q_2 + \frac{r_2}{r}}$, So in this way, the original $\frac{b}{a}$ becomes $\frac{1}{q+\frac{1}{q_2+\frac{r_2}{r}}}$. We continue doing this recursively, and we can get: $\frac{1}{q+\frac{1}{q_2+\frac{1}{q_3+\ldots+\frac{r_n}{rn-1}}}}$. We stop eventually when we get some remainder $r_n = 1$

We can use Euclid's algorithm to compute this fraction expansion:
Input: $a, b \in Z$ s.t. $a > b > 0$

```
set a_(0)=a, a_(1)=b, i=1
while (a_i is not 1) do:
    compute q_(i), q_(i+1) in Z, s.t. a_(i-1)=q_(i)*a_(i)+a(i+1)
    and 0 <= a(i+1) < a_(i)
    i++
end while
```

Output: Suppose the algorithm terminates when $i = j$, which is $a_j = 1$, we output the fraction expansion as :
$\frac{b}{a} = \frac{1}{q_1+\frac{1}{q_2+\frac{1}{q_3+\ldots+\frac{1}{q_j+\frac{1}{a_{j-1}}}}}}$