Yiluo Li
MATH 8
HW 4
30 Oct 2017

The Integers

Problem 1 For each of the following pairs a,b of integers,find the highest common factor d = hcf(a,b), and find integers s,t such that d = sa + tb:
(i) a=17, b=29.
(ii) a=552, b=713.
(iii) a=345, b=299.

(i)

$$\begin{aligned}
17 &= 29(0) + 17 \\
29 &= 17(1) + 12 \\
17 &= 12(1) + 5 \\
12 &= 5(2) + 2 \\
5 &= 2(2) + 1 \\
2 &= 1(2) + 0 \\
hcf(17,\ 29) &= \boxed{1} \\
1 &= 5 - 2(2) \\
1 &= 5 - 2(12 - 5(2)) \\
1 &= (17 - 12)(5) - 12(2) \\
1 &= (29 - 17)(-7) + 17(5) \\
1 &= \boxed{29(-7) + 17(12)}
\end{aligned}$$

■

(ii)

$$\begin{aligned}
552 &= 713(0) + 552 \\
713 &= 552(1) + 161 \\
552 &= 161(3) + 69 \\
161 &= 69(2) + 23 \\
69 &= 23(3) + 0 \\
hcf(552,\ 713) &= \boxed{23} \\
23 &= 161 - 69(2) \\
23 &= 161(7) - 552(2) \\
23 &= \boxed{713(7) - 552(9)}
\end{aligned}$$

■

(iii)

$$\begin{aligned}
345 &= 299(1) + 46 \\
299 &= 46(6) + 23 \\
46 &= 23(2) + 0 \\
hcf(345, 299) &= \boxed{23} \\
23 &= 299 - 46(6) \\
23 &= \boxed{299(7) - 345(6)}
\end{aligned}$$

■

Problem 3 A train leaves Moscow for St. Petersburg every 7 hours, on the hour. Show that on some days it is possible to catch this train at 9 a.m.
Whenever there is a 9 a.m. train, Ivan takes it to visit his aunt Olga. How often does Olga see her nephew?
Discuss the corresponding problem involving the train to Vladivostok, which leaves Moscow every 14 hours.

Part One

$$\begin{aligned}
hcf(24, 7) &= 1 \\
1 &= 24s + 7t
\end{aligned}$$

By having the above equation, we know that after every t trains and s days, the departing hour of the train will vary by 1 hour. Therefore, all hours (including 9 a.m) in a day will have a train departing on some day.

Part Two Suppose the first train leaves at 9 a.m., then the next time it will leave at 9 a.m. is after 24x hours. Because the train leaves every 7 hours, 24x is a multiple of 7, and x = 7. Therefore, after every 24 x 7 (a.k.a 7 days) hours, Olga can see her nephew.

Part Three

$$\begin{aligned}
hcf(14, 24) &= 2 \\
2 &= 24s + 14t
\end{aligned}$$

Therefore, when the train leaves on an odd hour on the first day, it will not leave on even hours after, vice versa. ■

Problem 5 (a) Let m, n be coprime integers, and suppose a is an integer which is divisible by both m and n. Prove that mn divides a. (b) Show that the conclusion of part (a) is false if m and n are not coprime (i.e., show that if m and n are not coprime, there exists an integer a such that m | a and n | a, but mn does not divide a).

Proof (a): Since m | a, we can write a = k_1m for some integer k_1. Since m is coprime with n, we can write:

$$\begin{aligned} 1 &= tm + sn \\ k_1 &= tk_1m + sk_1n \\ k_1 &= ta + sk_1n \end{aligned}$$

Since n | a, this equation can be $k_1 = k_2n$. Plug this back into $a = k_1m$ we get $a = k_2mn$. Therefore a is divisible by mn. ∎

(b): If m and n are not coprime, k = hcf(m, n) for some integer k $\geq$ 2. By letting m = ki, n = kj, we will get m | ijk and n | ijk, but mn $\nmid$ ijk. ∎

Prime Factorization

Problem 3 Suppose n $\geqslant$ 2 is an integer with the property that whenever a prime p divides n, p^2 also divides n (i.e., all primes in the prime factorization of n appear at least to the power 2). Prove that n can be written as the product of a square and a cube.

Proof:
($a^3b^2 \Rightarrow p^2 \mid n$)
Let $a^3b^2 = x$ for some a, b $\in \mathbb{Z}$, prove that x satisfies the property of n:
Integer a and b can be written as the product of primes:

$$x = (p_{a1}p_{a2}p_{a3}...p_{aj})^3(p_{b1}p_{b2}p_{b3}...p_{bk})^2$$

In which p_{aj} and p_{bk} represents prime factors of a and b. Notice that every unique prime numbers in the above equation repeats at least twice. Therefore, x divisible by any of the above prime number is also divisible by this prime number's square.

($a^3b^2 \Leftarrow p^2 \mid n$)
Let $n = p_1^2\ p_2^2\ ...\ p_n^2$ and let b equals to the product of all these primes $b = p_1\ p_2\ ...p_n$, and let a = 1. Then we can always write n in the form of $n = a^3b^2$ ∎

Problem 5 (a) Prove that $2^{\frac{1}{3}}$ and $3^{\frac{1}{3}}$ are irrational. (b) Let m and n be positive integers. Prove that $m^{\frac{1}{n}}$ is rational if and only if m is an n^{th} power (i.e., $m = c^n$ for some integer c).

Proof (a) part one: (**Proposition:** $2^{\frac{1}{3}}$ is irrational) By contradiction
Suppose $2^{\frac{1}{3}}$ is rational. Then we have $2^{\frac{1}{3}} = \frac{a}{b}$, for a, b $\in \mathbb{Z}$. After cubing both sides, we get $2b^3 = a^3$. We can write both a and b as products of primes:

$$\begin{aligned} a &= p_{a1}p_{a2}p_{a3}...p_{aj} \\ b &= p_{b1}p_{b2}p_{b3}...p_{bk} \end{aligned}$$

In which $p_{a1} = 2^x$ and $p_{b1} = 2^y$ for x, y $\in \mathbb{Z}$. Therefore we can write the cube function as following:

$$2(2^y p_{b2} p_{b3} ... p_{bk})^3 = (2^x p_{a2} p_{a3} ... p_{aj})^3$$

Since $p_b k \neq 2$ and $p_a j \neq 2$ for j,k ≥ 2, the following relation can be derived from the above equation:

$$3y + 1 = 3x$$

This cannot be possible since x, y $\in \mathbb{Z}$. Therefore, this is a contradiction. ∎

Proof (a) part two: (This is pretty much exactly the same as above)
(**Proposition:** $3^{\frac{1}{3}}$ is irrational) By contradiction
Suppose $3^{\frac{1}{3}}$ is rational. Then we have $3^{\frac{1}{3}} = \frac{a}{b}$, for a, b $\in \mathbb{Z}$. After cubing both sides, we get $3b^3 = a^3$. We can write both a and b as products of primes:

$$a = p_{a1} p_{a2} p_{a3} ... p_{aj}$$
$$b = p_{b1} p_{b2} p_{b3} ... p_{bk}$$

In which $p_{a1} = 3^x$ and $p_{b1} = 3^y$ for x, y $\in \mathbb{Z}$. Therefore we can write the cube function as following:

$$3(3^y p_{b2} p_{b3} ... p_{bk})^3 = (3^x p_{a2} p_{a3} ... p_{aj})^3$$

Since $p_b k \neq 3$ and $p_a j \neq 3$ for j,k ≥ 2, the following relationship can be derived from the above equation:

$$3y + 1 = 3x$$

This cannot be possible since x, y $\in \mathbb{Z}$. Therefore, this is a contradiction. ∎

Proof (b):
($m^{\frac{1}{n}}$ *is rational* $\Rightarrow m = c^n$, $c \in \mathbb{Z}$)
We want to prove that m has the form $m = c^{xn}$ for some c, x$\in \mathbb{Z}$.
Suppose $m^{\frac{1}{n}}$ is rational, so we can write it in the form of

$$m^{\frac{1}{n}} = \frac{a}{b}$$
$$b^n m = a^n$$

Now we can write a, b, m in the form of respective highest powers of a same prime that divide them p^i, p^j, p^k:

$$p^{jn} p^k = d^{in}$$
$$k = in - jn$$
$$k = (i - j)n$$

Therefore, m has the form of $m = c^{xn}$ in which x = (i - j).

$(m^{\frac{1}{n}}$ *is rational* $\Leftarrow m = c^n,\ c \in \mathbb{Z})$
Since we have $m = c^n$, $m^{\frac{1}{n}} = c$, and c is rational. ∎

Problem 6 Let E be the set of all positive even integers. We call a number e in E prima if e cannot be expressed as a product of two other members of E.
(i) Show that 6 is prima but 4 is not.
(ii) What is the general form of a prima in E?
(iii) Prove that every element of E is equal to a product of primas.
(iv) Give an example to show that E does not satisfy a unique prima factorization theorem (i.e., find an element of E that has two different factorizations as a product of primes).

(i) The prime factors for 6 are 2, 3. There is only one even prime factor, so the combination of factors for 6 will only contain one even number. Therefore, it is prima. However, 4 can be expressed as 2 x 2, so it is not prima. ∎

(ii) The prima r in E will have the general form as following:

$$r = 2p_1p_2p_3...p_n$$

In which $p_n \neq 2$ for all n. ∎

(iii) Every element e of E is an even number, and can therefore be written as e = 2^nk for some n, k $\in \mathbb{Z}$. 2 is a prima because it only has factors 1 and 2. Since k is an integer, we can write it in the form:

$$k = p_1p_2p_3...p_n$$

Such that $p_n \neq 2$ for all n. 2k will be a prima, and the rest of 2's are also primas. Therefore, every element of E is equal to a product of primas. ∎

(iv) If we have 180, it can be written as the product of 30 and 6, both primas, or 10 and 18, also both primas. ∎

Problem 8 Find all solutions $x, y \in \mathbb{Z}$ to the following Diophantine equations:
(a) $x^2 = y^3$.
(b) $x^2 - x = y^3$.
(c) $x^2 = y^4 - 77$.
(d) $x^3 = 4y^2 + 4y - 3$.

(a) Let p be a prime and p^a, p^b be the highest powers of prime that divides x and y respectively. Then we can write the Diophantine equation as:

$$\begin{aligned} p^{2a} &= p^{3b} \\ 2a &= 3b \\ \frac{a}{b} &= \frac{3}{2} \end{aligned}$$

The solution to this equation will have numbers of the same prime factor satisfy the above relation. (e.g. if p is a prime factor of x, then p^3 will factor x as well while p^2 will factor y.)

■

(b) $x^2 - x$ can be written as $x(x-1)$, in which x and (x - 1) are always coprime. Therefore, from the conclusion of previous question, for every prime factor p_x for x and p_{x-1} for (x - 1), p^3 and p_{x-1}^3 must also be a factor of x and (x - 1) respectively. ■

(c) I didn't really find a good way to prove it.

$$\begin{aligned} x = \pm 2,\ y = 3 \\ x = \pm 2,\ y = -3 \end{aligned}$$

■

■