M328K: Homework 5

Katherine Ho

October 15, 2024

1. Calculate $\text{lcm}(140, 520)$.

   Proof. First,
   $$\text{lcm}(140, 520) = \frac{140 \cdot 520}{\gcd(140, 520)}$$
   We can use the Euclidean Algorithm to solve for $\gcd(140, 520)$.
   $$\begin{aligned} 520 &= 140(3) + 100 \\ 140 &= 100(1) + 40 \\ 100 &= 40(2) + 20 \\ 40 &= 20(2) + 0 \\ \gcd(140, 520) &= 20 \end{aligned}$$
   Then by substitution,
   $$\text{lcm}(140, 520) = \frac{140 \cdot 520}{\gcd(140, 520)} = \frac{72800}{20} = 3640$$
   □

2. (a) Let m and n be relatively prime positive integers. Show that every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $\gcd(d_1, d_2) = 1$.

   Proof. Let $m = (p_1^{a_1}) \dots (p_i^{a_i})$ be the prime factorization of m. Let $n = (q_1^{b_1}) \dots (q_i^{b_i})$ be the prime factorization of n. Given m and n are relatively prime, m and n do not share any factors. Thus each term p_i and q_i is distinct. So, we can say the prime factorization of mn is
   $$mn = (p_1^{a_1}) \dots (p_i^{a_i}) \cdot (q_1^{b_1}) \dots (q_i^{b_i})$$
   If d is a divisor of mn, then
   $$d = (p_1^{c_1}) \dots (p_i^{c_i}) \cdot (q_1^{e_1}) \dots (q_i^{e_i})$$
   where $0 \leq c_i \leq a_i$ and $0 \leq e_i < b_i$. Let $d_1 = (p_1^{c_1}) \dots (p_i^{c_i})$ and let $d_2 = (q_1^{e_1}) \dots (q_i^{e_i})$. d_1 is a divisor of m and d_2 is a divisor of n since $0 \leq c_i \leq a_i$ and $0 \leq e_i < b_i$. They are coprime since every term p_i and q_i is distinct. From this we can see that d is the product of a divisor of m and a divisor of n. This product is unique since it is the unique prime factorization of d. Thus every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $\gcd(d_1, d_2) = 1$.
   □

(b) Show that if f is a multiplicative function and F is defined by

$$F(n) = \sum_{d|n} f(d)$$

then F is also multiplicative.

Hint: Here's a concrete case that illustrates how to use the result from part (a) in the proof.

$$\begin{aligned} F(3 \cdot 4) &= \sum_{d|12} f(d) \\ &= f(1) + f(2) + f(3) + f(4) + f(6) + f(12) \\ &= f(1 \cdot 1) + f(1 \cdot 2) + f(3 \cdot 1) + f(1 \cdot 4) + f(3 \cdot 2) + f(3 \cdot 4) \\ &= f(1)f(1) + f(1)f(2) + f(3)f(1) + f(1)f(4) + f(3)f(2) + f(3)f(4) \\ &= \Big(f(1) + f(3)\Big)\Big(f(1) + f(2) + f(4)\Big) \\ &= F(3)F(4). \end{aligned}$$

Proof. To show that F is multiplicative, we want to show that $F(mn) = F(m)F(n)$.

$$F(mn) = \sum_{d|mn} f(d)$$

We can say $d = d_1 \cdot d_2$ where d_1 is a divisor of n and d_2 is a divisor of m. And since f is multiplicative, we have

$$\begin{aligned} \sum_{d|mn} f(d) &= \sum_{d_1|n} \sum_{d_2|m} f(d_1)f(d_2) \\ &= \sum_{d_1|n} [f(d_1) \cdot \sum_{d_2|m} f(d_2)] \\ &= \sum_{d_1|n} [f(d_1) \cdot F(m)] \\ &= F(m) \sum_{d_1|n} f(d_1) \\ &= F(m)F(n) \end{aligned}$$

Now we have

$$F(mn) = F(m)F(n)$$

Thus if f is a multiplicative function and F is defined by

$$F(n) = \sum_{d|n} f(d)$$

then F is also multiplicative. □

3. Show that $\displaystyle\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ for every positive integer n.

Hint: If you want to show that two multiplicative functions f and g are the same, it is enough to show that $f(p^k) = g(p^k)$ for prime powers p^k.

Proof.

$$\begin{aligned}\sigma(n) &= \sum_{d|n} d \\ &= \sum_{d|n} \frac{n}{d} \\ &= n \sum_{d|n} \frac{1}{d} \\ \frac{\sigma(n)}{n} &= \sum_{d|n} \frac{1}{d}\end{aligned}$$

□

4. Given that 3 is a primitive root of 43, find all positive integers n less than 43 such that

   (a) $\text{ord}(n) = 6$.

   Proof. Given that 3 is a primitive root of 43, then $\text{ord}_{43}(3) = \phi(43)$. Since 43 is prime, $\phi(43) = 43 - 1 = 42$. So, $\text{ord}_{43}(3) = 42$. Then,

   $$\text{ord}_{43}(3^h) = \frac{42}{\gcd(h, 42)}$$

   Since we want to find n such that $\text{ord}(n) = 6$, we need to find the integers h that satisfy the following where $n = 3^h \pmod{43}$.

   $$\begin{aligned}\frac{42}{\gcd(h, 42)} &= 6 \\ 7 &= \gcd(h, 42) \\ h &= 7, 35\end{aligned}$$

   With substitution, $n = 3^7 \pmod{43}$ and $n = 3^{35} \pmod{43}$.

   $$\begin{aligned}n = 3^7 \pmod{43} &= 2187 \pmod{43} \equiv 37 \\ n = 3^{35} \pmod{43} &= (3^7)^5 \pmod{43} \equiv 37^5 \pmod{43} \equiv 7\end{aligned}$$

   Thus $n = 7, 37$. □

   (b) $\text{ord}(n) = 21$.

   Proof. Since we want to find n such that $\text{ord}(n) = 21$, we need to find the integers h that satisfy the following where $n = 3^h$.

   $$\begin{aligned}\frac{42}{\gcd(h, 42)} &= 21 \\ 2 &= \gcd(h, 42) \\ h &= 2, 4, 8, 10, 16, 20, 22, 26, 32, 34, 38, 40\end{aligned}$$

By substitution, we have

$$\begin{aligned}
n &= 3^2 \pmod{43} \equiv 9 \\
n &= 3^4 \pmod{43} \equiv 38 \\
n &= 3^8 \pmod{43} \equiv 25 \\
n &= 3^{10} \pmod{43} \equiv 10 \\
n &= 3^{16} \pmod{43} \equiv 23 \\
n &= 3^{20} \pmod{43} \equiv 14 \\
n &= 3^{22} \pmod{43} \equiv 40 \\
n &= 3^{26} \pmod{43} \equiv 15 \\
n &= 3^{32} \pmod{43} \equiv 13 \\
n &= 3^{34} \pmod{43} \equiv 31 \\
n &= 3^{38} \pmod{43} \equiv 17 \\
n &= 3^{40} \pmod{43} \equiv 24
\end{aligned}$$

Thus $n = 9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40$. □

(c) n is a primitive root of 43.

Proof. Given 3 is a primitive root, $\text{ord}_{43}(3) = \phi(43) = 42$. Also,

$$\text{ord}_{43}(3^h) = \frac{42}{\gcd(h, 42)}$$

3^h is a primitive root $\pmod{43}$ if $\text{ord}_{43}(3^h) = 42$. So, find all values of h such that $\gcd(h, 42) = 1$.

$$h = 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$$

Now find $3^h \pmod{43}$ for all values of h.

$$\begin{aligned}
3^1 &\pmod{43} = 3 \\
3^5 &\pmod{43} = 28 \\
3^{11} &\pmod{43} = 30 \\
3^{13} &\pmod{43} = 12 \\
3^{17} &\pmod{43} = 26 \\
3^{19} &\pmod{43} = 19 \\
3^{23} &\pmod{43} = 34 \\
3^{25} &\pmod{43} = 5 \\
3^{29} &\pmod{43} = 18 \\
3^{31} &\pmod{43} = 33 \\
3^{37} &\pmod{43} = 20 \\
3^{41} &\pmod{43} = 29
\end{aligned}$$

So, the primitive roots of 43 are $3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 34, 33$. □

5. Suppose $n = pq$ is the product of two distinct odd primes. Show that $\text{ord}_n(a)$ divides $\phi(n)/2$ for all a relatively prime to n and hence that there is no "primitive root of pq".

Proof. First, $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$. A positive integer x has a primitive root iff $x = 2, 4, p^k$, or $2p^k$. Since n is the product of distinct odd primes p and q, n cannot fit the criteria to have a primitive root.

□