MATH 324 Summer 2006
Elementary Number Theory
Solutions to Assignment 5
Due: Thursday August 17, 2006

Department of Mathematical and Statistical Sciences
University of Alberta

Question 1. [p 246. #21]

Show that if m and n are positive integers and $(m, n) = p$, where p is prime, then

$$\phi(m\,n) = \frac{p\,\phi(m)\,\phi(n)}{p-1}.$$

SOLUTION: Since $(m, n) = p$, then $p \mid m$ and $p \mid n$, and p divides one of the two integers m and n exactly once, otherwise $(m, n) \geq p^2$, which is a contradiction.

Assume that $p \mid n$ but $p^2 \nmid n$, then there exists an integer k such that $n = kp$ and $(k, p) = 1$, and since $p = (m, n)$, then $(m, k) = 1$ also, and therefore

$$\phi(n) = \phi(kp) = \phi(k)\phi(p) = \phi(k)(p-1).$$

Now, if $m = p^{\alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime power decomposition of m, then

$$\begin{aligned}\phi(mp) &= p^{\alpha}(p-1)p^{\alpha_1-1}(p_1-1)\cdots p_r^{\alpha_r-1}(p_r-1)\\ &= p \cdot p^{\alpha-1}(p-1)p^{\alpha_1-1}(p_1-1)\cdots p_r^{\alpha_r-1}(p_r-1)\\ &= p\cdot\phi(m),\end{aligned}$$

so that

$$\phi(mp) = p\phi(m),$$

and

$$\phi(mn) = \phi(mkp) = \phi(mp)\phi(k) = \frac{p\phi(m)\phi(n)}{p-1}.$$

Question 2. [p 246. #22]

Show that if m and k are positive integers, then

$$\phi(m^k) = m^{k-1}\phi(m).$$

SOLUTION: Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the prime power decomposition of m, then

$$\phi(m) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_r^{\alpha_r-1}(p_r-1).$$

Since $m^k = p_1^{k\alpha_1} p_2^{k\alpha_2} \cdots p_r^{k\alpha_r}$, then

$$\begin{aligned}\phi(m^k) &= p_1^{k\alpha_1-1}(p_1-1)p_2^{k\alpha_2-1}(p_2-1)\cdots p_r^{k\alpha_r-1}(p_r-1)\\ &= p_1^{(k-1)\alpha_1+\alpha_1-1}(p_1-1)p_2^{(k-1)\alpha_2+\alpha_2-1}(p_2-1)\cdots p_r^{(k-1)\alpha_r+\alpha_r-1}(p_r-1)\\ &= p_1^{(k-1)}p_1^{\alpha_1-1}(p_1-1)p_2^{(k-1)}p_2^{\alpha_2-1}(p_2-1)\cdots p_r^{(k-1)}p_r^{\alpha_r-1}(p_r-1)\\ &= m^{k-1}p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_r^{\alpha_r-1}(p_r-1)\\ &= m^{k-1}\phi(m),\end{aligned}$$

so that $\phi(m^k) = m^{k-1}\phi(m)$.

Question 3. [p 246. #23]

Show that if a and b are positive integers and $d = (a, b)$, then

$$\phi(a\,b) = \frac{d\,\phi(a)\,\phi(b)}{\phi(d)}.$$

Conclude that if $d > 1$, then $\phi(a\,b) > \phi(a)\,\phi(b)$.

SOLUTION: Let $p_1, p_2, \ldots, p_r$ be those primes dividing a but not b, let $q_1, q_2, \ldots, q_s$ be those primes dividing b but not a, and let $r_1, r_2, \ldots, r_t$ be those primes dividing both a and b.

Define

$$P = \prod_{k=1}^{r}\left(1 - \frac{1}{p_k}\right), \qquad Q = \prod_{k=1}^{s}\left(1 - \frac{1}{q_k}\right), \qquad \text{and} \qquad R = \prod_{k=1}^{t}\left(1 - \frac{1}{r_k}\right),$$

then

$$\phi(a\,b) = abPQR = \frac{aPR\,bQR}{R} = \frac{\phi(a)\phi(b)}{R}.$$

However,

$$\phi\left((a, b)\right) = (a, b)R$$

so that

$$R = \frac{\phi(d)}{d}$$

since $d = (a, b)$, and therefore

$$\phi(a\,b) = \frac{d\,\phi(a)\,\phi(b)}{\phi(d)}.$$

Note that if $d > 1$, then $\phi(d) \le d - 1 < d$, so that

$$\frac{d}{\phi(d)} > 1,$$

and

$$\phi(a\,b) = \frac{d\,\phi(a)\,\phi(b)}{\phi(d)} > \phi(a)\,\phi(b).$$

Question 4. [p 247. #30]

Show that if n is a positive integer with $n \neq 2$ and $n \neq 6$, then $\phi(n) \ge \sqrt{n}$.

SOLUTION: Note first that if p is an odd prime and $\alpha > 1$, then

$$\phi(p) = p - 1 > \sqrt{p}$$

and

$$\phi(2p^\alpha) = \phi(2)\phi(p^\alpha) = p^{\alpha-1}(p-1) \ge 2p^{\alpha-1} \ge 2p^{\frac{\alpha}{2}} \ge \sqrt{2p^\alpha}.$$

Now let p be any prime and let $\alpha > 1$, then

$$\phi(p^\alpha) = p^{\alpha-1}(p-1) \ge p^{\alpha-1} \ge p^{\frac{\alpha}{2}} = \sqrt{p^\alpha}$$

and the result is true for any prime power p^α with $\alpha > 1$.

Now, if p is any prime with $p > 4$, then $p^2 + 1 > 4p$, so that

$$(p-1)^2 = p^2 - 2p + 1 > 4p - 2p = 2p,$$

and

$$\phi(2p) = p - 1 \geq \sqrt{2p}.$$

Now let n be a positive integer, and suppose the prime power decomposition of n is given by

$$n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

if $\alpha_0 \neq 1$, since the ϕ-function and the square root function are both multiplicative, from the results above, we have

$$\phi(n) = \prod_{k=0}^{r} \phi(p_k^{\alpha_k}) \geq \prod_{k=0}^{r} \sqrt{p_k^{\alpha_k}} = \sqrt{n}.$$

If $\alpha_0 = 1$, be rearranging the primes, we may assume that $p_1^{\alpha_1}$ has either $\alpha_1 > 1$ or $p_1 > 4$, and again since the ϕ-function and the square root function are both multiplicative, from the results above, we have

$$\phi(n) = \phi(2p_1^{\alpha_1}) \prod_{k=2}^{r} \phi(p_k^{\alpha_k}) \geq \sqrt{2p_1^{\alpha_1}} \prod_{k=2}^{r} \sqrt{p_k^{\alpha_k}} = \sqrt{n}.$$

The only remaining cases are when n is exactly divisible by 2, not divisible by a prime greater than 4, and not divisible by a prime to a power greater than 1. These are exactly the cases $n = 2$ and $n = 6$, which are the only exceptions.

Question 5. [p 247. #32]

Show that if m and n are positive integers with $m \mid n$, then $\phi(m) \mid \phi(n)$.

Solution: Let m and n be positive integers and suppose that $m \mid n$, if the prime power decomposition of n is given by

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

then the prime power decomposition of m is given by

$$m = p_{i_1}^{\beta_1} p_{i_2}^{\beta_2} \cdots p_{i_s}^{\beta_s},$$

where $1 \leq \beta_k \leq \alpha_{i_k}$ for $1 \leq k \leq s$.

Therefore,

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$$

and

$$\phi(m) = p_{i_1}^{\beta_1 - 1}(p_{i_1} - 1) p_{i_2}^{\beta_2 - 1}(p_{i_2} - 1) \cdots p_{i_s}^{\beta_s - 1}(p_{i_s} - 1),$$

where $1 \leq \beta_k \leq \alpha_{i_k}$ for $1 \leq k \leq s$, and clearly $\phi(m) \mid \phi(n)$.

Question 6. [p 253. #4]

For which positive integers n is the sum of divisors of n odd?

SOLUTION: We will show first that $\sigma(n)$ is odd if n is a power of 2. Suppose that $n = 2^\alpha$, then

$$\sigma\left(2^\alpha\right) = \sum_{d \mid 2^\alpha} d = 1 + 2 + 2^2 + \cdots + 2^\alpha = \frac{2^{\alpha+1} - 1}{2 - 1} = 2^{\alpha+1} - 1,$$

and $\sigma\left(2^\alpha\right) = 2^{\alpha+1} - 1$ is odd for all integers $\alpha \geq 0$.

Next suppose that p is an odd prime and that α is a positive integer, then

$$\sigma\left(p^\alpha\right) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1},$$

and $\sigma\left(p^\alpha\right)$ is odd if and only if the sum contains an odd number of terms, that is, if and only if α is an even integer.

From the Fundamental Theorem of Arithmetic, we see that $\sigma(n)$ is odd if and only if in the prime power decomposition of n, every odd prime occurs to an even power, that is, if and only if n is perfect square or n is 2 times a perfect square.

Question 7. [p 254. #21, #22, #23]

Let $\sigma_k(n)$ denote the sum of the kth powers of the divisors of n, so that

$$\sigma_k(n) = \sum_{d \mid n} d^k.$$

(a) Find a formula for $\sigma_k(p)$, where p is a prime.

(b) Find a formula for $\sigma_k(p^\alpha)$, where p is a prime and α is a positive integer.

(c) Show that the arithmetic function σ_k is multiplicative.

SOLUTION:

(a) If p is a prime, then

$$\sigma_k(p) = 1 + p^k = \frac{p^{2k} - 1}{p^k - 1}$$

since the only positive divisors of p are 1 and p itself.

(b) If p is a prime and α is a positive integer, then

$$\sigma_k(p^\alpha) = \sum_{d \mid p^\alpha} d^k = \sum_{i=0}^{\alpha} p^{ki} = \frac{p^{k(\alpha+1)} - 1}{p^k - 1}$$

since the positive divisors of p^α are $1, p, \ldots, p^\alpha$.

(c) Define the arithmetic function $f_k(n) = n^k$, then f is multiplicative, since if $(m, n) = 1$, then

$$f_k(mn) = (mn)^k = m^k n^k = f_k(m) f_k(n).$$

Therefore the function

$$\sigma_k(n) = \sum_{d \mid n} d^k$$

is also multiplicative.

Question 8. [p 254. #27]

Show that the number of ordered pairs of positive integers with least common multiple equal to the positive integer n is $\tau(n^2)$.

Solution: Clearly the result is true if $n = 1$, since then $\tau(n^2) = 1$, and the only ordered pair of positive integers with least common multiple 1 is $(1, 1)$.

Let n be a positive integer with $n > 1$, and suppose the prime power decomposition of n is given by

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

where $p_1 < p_2 < \cdots < p_r$ are distinct primes and $\alpha_k \geq 1$ for $1 \leq k \leq r$.

Now suppose that b and c are positive integers such that $[b, c] = n$, then $b \mid n$ and $c \mid n$, so that their prime power decompositions are given by

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \qquad \text{and} \qquad c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$$

where $0 \leq \beta_k \leq \alpha_k$ and $0 \leq \gamma_k \leq \alpha_k$ for $1 \leq k \leq r$.

Since $[b, c] = n$, then we must have $\max\{\beta_k, \gamma_k\} = \alpha_k$ for $1 \leq k \leq r$, so that for each such k, one of β_k or γ_k must be equal to α_k, while the other can be any one of the integers $0 \leq \ell \leq \alpha_k$.

Therefore, for each k with $1 \leq k \leq r$, the number of ways to choose the ordered pair (β_k, γ_k) such that exactly one or both of β_k and γ_k equals α_k is equal to

$$\alpha_k + \alpha_k + 1 = 2\alpha_k + 1,$$

and the number of ways to choose the exponents

$$\beta_1,\, \beta_2,\, \ldots,\, \beta_r,\, \gamma_1,\, \gamma_2,\, \ldots,\, \gamma_r$$

is equal to

$$(2\alpha_1 + 1)(2\alpha_2 + 1) \cdots (2\alpha_r + 1) = \tau(n^2).$$

Thus, the number of ordered pairs of positive integers (b, c) such that $[b, c] = n$ is equal to $\tau(n^2)$.

Question 9. [p 256. #34]

Show that if n is a positive integer, then

$$\left(\sum_{d|n} \tau(d) \right)^2 = \sum_{d|n} \tau(d)^3.$$

Solution: Let

$$F(n) = \left(\sum_{d \mid n} \tau(d) \right)^2 \qquad \text{and} \qquad G(n) = \sum_{d \mid n} \tau(d)^3$$

for $n \geq 1$, then F and G are multiplicative since τ is multiplicative, and in order to show that the equality $F(n) = G(n)$ holds for all $n \geq 1$, we need only show it is true for $n = p^\alpha$ where p is a prime and $\alpha \geq 1$.

Now, the divisors of p^α are $1, p, p^2, \cdots, p^\alpha$, and

$$\tau(1) = 1,\ \tau(p) = 2,\ \tau(p^2) = 3,\ \ldots,\ \tau(p^\alpha) = \alpha + 1,$$

so that

$$F(p^\alpha) = \left(\sum_{k=1}^{\alpha+1} k\right)^2 = \sum_{k=1}^{\alpha+1} k^3 = G(p^\alpha).$$

Question 10. [p 256. #35]

Show that if n is a positive integer, then

$$\tau(n^2) = \sum_{d|n} 2^{\,\omega(d)},$$

where $\omega(n)$ equals the number of prime divisors of n.

Solution: Let $\omega(n)$ be the number of distinct primes dividing the positive integer n, we will show that $\omega(n)$ is an *additive* function, in the sense that it satisfies

$$\omega(mn) = \omega(m) + \omega(n)$$

whenever m and n are relatively prime positive integers.

To see this, suppose that $(m, n) = 1$, and the prime power decompositions of m and n are given by

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \qquad \text{and} \qquad n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

where $p_1 < p_2 < \cdots < p_r$ and $q_1 < q_2 < \cdots < q_s$ are distinct primes, with $p_i \neq q_j$ for any i and j, and $\alpha_i \geq 1$, $\beta_j \geq 1$ for all i and j.

The prime power decomposition of mn is given by

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

and clearly

$$\omega(mn) = r + s = \omega(m) + \omega(n).$$

From the above we see that

$$f(n) = 2^{\omega(n)}$$

is multiplicative, since if m and n are relatively prime, then

$$f(mn) = 2^{\omega(mn)} = 2^{\omega(m)+\omega(n)} = 2^{\omega(m)} 2^{\omega(n)} = f(m)f(n).$$

Therefore,

$$F(n) = \sum_{d|n} 2^{\omega(d)}$$

is multiplicative.

Now let $G(n) = \tau(n^2)$, then G is multiplicative, since if $(m,n) = 1$, then $(m^2, n^2) = 1$ also, and

$$G(mn) = \tau(m^2n^2) = \tau(m^2)\tau(n^2) = G(m)G(n).$$

Since F and G are multiplicative, in order to show that $F(n) = G(n)$ for all $n \geq 1$, we need only show that $F(p^\alpha) = G(p^\alpha)$ whenever p is a prime and α is a positive integer.

Let p be a prime and $\alpha \geq 1$, then

$$F(p^\alpha) = \sum_{d \mid p^\alpha} 2^{\omega(d)} = \sum_{k=0}^{\alpha} 2^{\omega(p^k)} = 1 + \sum_{k=1}^{\alpha} 2^1 = 2\alpha + 1$$

since $\omega(p^0) = \omega(1) = 0$, while

$$\tau\left((p^\alpha)^2\right) = \tau(p^{2\alpha}) = 2\alpha + 1.$$

Therefore, from the fundamental theorem of arithmetic we have

$$\tau(n^2) = \sum_{d \mid n} 2^{\,\omega(d)}$$

for all $n \geq 1$.