Homework #9 Solutions

7.1.8. Suppose n is a positive integer such that $\varphi(n) = 14 = 2 \cdot 7$. Since $\varphi(2^a) = 2^{a-1}$ for any integer $a \geq 1$, n cannot be a power of 2. Therefore n must have an odd prime divisor p. If n has a second odd prime divisor, say q, then the product formula for φ implies that $(p-1)(q-1)$ divides $\varphi(n) = 14$. However, as both $p-1$ and $q-1$ are even, this forces 4 to divide 14, a contradiction. Therefore $n = 2^a p^b$ for integers $a \geq 0$ and $b \geq 1$, and $\varphi(n) = 2^{a-1}p^{b-1}(p-1)$. We must then have $a \leq 1$ since otherwise $14 = \varphi(n)$ would be divisible by 4 as above. If n is even, then $\varphi(n/2) = \varphi(n) = 14$, so, replacing n with $n/2$ if necessary, we may assume that $n = p^b$ for an odd prime p and an integer $b \geq 1$, and we have $14 = \varphi(n) = p^{b-1}(p-1)$. If $b > 1$, then $p \mid 14$, so $p = 7$ and $6 = p - 1$ divides 14, a contradiction. This means $b = 1$, from which it follows that $14 = \varphi(n) = p - 1$, and thus $p = 15$, which is totally ridiculous, and I am vaguely insulted that you have suggested it. So no such n can exist.

7.1.14. Let n have prime factorization $n = p_1^{e_1} p_2^{e_1} \cdots p_r^{e_r}$. Using the product formula for φ, we see that $\varphi(n)$ divides n if and only if

$$\frac{n}{\varphi(n)} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)^{-1} = \prod_{i=1}^{r} \frac{p_i}{p_i - 1}$$

is an integer. We assume that this is the case. Each odd prime factor of n contributes at least one factor of 2 to the denominator of the rational number $n/\varphi(n)$, but the numerator of $n/\varphi(n)$ has at most one factor of 2. Therefore n can have at most one odd prime divisor, so we may write $n = 2^a p^b$ for an odd prime p and nonnegative integers a and b. If $a = 0$ and $b \geq 1$, then

$$\frac{n}{\varphi(n)} = \frac{p}{p-1},$$

which is not an integer as p is odd, so either $a \geq 1$ or $b = 0$. When $b \geq 1$ (and so necessarily $a \geq 1$ as well), we have

$$\frac{n}{\varphi(n)} = 2\frac{p}{p-1} = \frac{2p}{p-1}.$$

As $n/\varphi(n)$ is an integer, it follows that $p-1$ divides $2p$, and since $(p, p-1) = 1$, $p-1$ divides 2, which forces $p = 3$. Thus the possibilities are $n = 1$, $n = 2^a$ for $a \geq 1$, and $n = 2^a 3^b$ for $a, b \geq 1$. Conversely, it can be verified that $n/\varphi(n)$ is an integer for each of these possibilities. Namely, when $n = 1$, $n = \varphi(n) = 1$, when $n = 2^a$ for $a \geq 1$, $n/\varphi(n) = 2^a/2^{a-1} = 2$, and when $n = 2^a 3^b$ for $a, b \geq 1$, $n/\varphi(n) = 3$. We have therefore identified all of the positive integers n for which $\varphi(n)$ divides n.

7.1.20. If p does not divide n, then, as p is prime, $(p, n) = 1$, so, by the multiplicativity of φ, $\varphi(pn) = \varphi(p)\varphi(n) = (p-1)\varphi(n)$. Assume now that p divides n, and write $n = p^e m$ with $e \geq 1$ and $(p, m) = 1$. We then have

$$\varphi(pn) = \varphi(p^{e+1}m) = \varphi(p^{e+1})\varphi(m) = p^e(p-1)\varphi(m),$$

Date: April 12, 2018.

while

$$\begin{aligned}(p-1)\varphi(n) &= (p-1)\varphi(p^e m)\\ &= (p-1)\varphi(p^e)\varphi(m)\\ &= (p-1)p^{e-1}(p-1)\varphi(m) = p^{e-1}(p-1)^2\varphi(m).\end{aligned}$$

Thus $\varphi(pn)/((p-1)\varphi(n)) = p/(p-1) \neq 1$, i.e., $\varphi(pn) \neq (p-1)\varphi(n)$. Therefore, if $\varphi(pn) = (p-1)\varphi(n)$, then it must be that $p \nmid n$.

7.1.22. Let m have prime factorization $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, so that m^k has prime factorization $p_1^{e_1k}p_2^{e_2k}\cdots p_r^{e_rk}$. We therefore have

$$\varphi(m^k) = m^k\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) = m^{k-1}\left(m\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\right) = m^{k-1}\varphi(m).$$

So we win.

7.1.27. For a prime p and a positive integer m, we denote by $v_p(m)$ the exponent of p in the prime factorization of m. Let n be any positive integer with $\varphi(n) = k$. Then, using the multiplicativity of φ, we have that $p^{v_p(n)-1}(p-1) \mid k$. Therefore $p^{v_p(n)-1} \mid k$ and $p-1 \mid k$. The first divisibility implies that $v_p(n)-1 \leq v_p(k)$, or equivalently, that $v_p(n) \leq v_p(k)+1$. The second divisibility implies that $p-1 \leq k$, or equivalently, that $p \leq k+1$. Therefore n can only be divisible by the finitely many primes not exceeding $k+1$, and the possible multiplicities of these primes in n are bounded independently of n (namely, by one plus the multiplicity of the corresponding prime in k). By unique factorization, there are only finitely many such positive integers n, and thus only finitely many positive integers n satisfying $\varphi(n) = k$.

7.2.40. Since φ is multiplicative by Theorem 7.4, Theorem 7.8 implies that the summatory function F of φ, given by $F(n) = \sum_{d\mid n}\varphi(d)$, is also multiplicative. We wish to show that $F(n) = n$ for all positive integers n. Observe that, if n has prime factorization $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, then, by multiplicativity of F,

$$F(n) = F(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}) = F(p_1^{e_1})F(p_2^{e_2})\cdots F(p_r^{e_r}),$$

and it therefore suffices to show that $F(p^e) = p^e$ for a prime p and a positive integer e (we are omitting $n = 1$ here, but it is clear that $F(1) = 1$ (this is not a proof by intimidation, as the fact that $F(1) = 1$ really is clear, objectively)). We will prove the necessary formula by induction on e. When $e = 1$, since the divisors of $p^e = p$ are 1 and p, we have

$$F(p) = \varphi(1) + \varphi(p) = 1 + p - 1 = p.$$

Assume now that for some integer $e \geq 1$, we have $F(p^e) = p^e$. The divisors of p^{e+1} are the powers p^i with $0 \leq i \leq e+1$, so we then have

$$\begin{aligned}F(p^{e+1}) &= \sum_{i=0}^{e+1}\varphi(p^i)\\ &= \left(\sum_{i=0}^{e}\varphi(p^i)\right) + \varphi(p^{e+1})\\ &= F(p^e) + p^{e+1} - p^e = p^e + p^{e+1} - p^e = p^{e+1}.\end{aligned}$$

So, by induction, $F(p^e) = p^e$ for all integers $e \geq 1$, completing the proof.