Math 25: Solutions to Homework # 5

(6.2 # 8) Show that if p is prime and $2^p - 1$ is composite, then $2^p - 1$ is a pseudoprime to the base 2.

Let $m = 2^p - 1$. Since p is prime, $2^p \equiv 2 \pmod{p}$, so $p \mid 2^p - 2$, hence $2^p - 2 = kp$ for some integer k. Then $2^{m-1} = 2^{2^p-2} = 2^{kp}$. Now $m = 2^p - 1 \mid 2^{kp} - 1 = 2^{m-1} - 1$, so $2^{m-1} \equiv 1 \pmod{m}$. Therefore, $m = 2^p - 1$ is a pseudoprime to the base 2.

(6.2 # 10) Suppose that a and n are relatively prime positive integers. Show that if n is a pseudoprime to the base a, then n is a pseudoprime to the base $\overline{a}$, where $\overline{a}$ is an inverse of a modulo n.

Let $\overline{a}$ be an inverse of a modulo m. Then since $a^{n-1} \equiv 1 \pmod{n}$,

$$(\overline{a})^{n-1} \equiv a^{n-1}(\overline{a})^{n-1} \equiv (a\overline{a})^{n-1} \equiv 1^{n-1} \equiv 1 \pmod{n},$$

so n is a pseudoprime to the base $\overline{a}$.

(6.2 # 12) Show that 25 is a strong pseudoprime to the base 7.

We can write $25 - 1 = 24 = 2^3 \cdot 3$. Then

$$7^{2\cdot 3} \equiv (7^2)^3 \equiv (49)^3 \equiv (-1)^3 \equiv -1 \pmod{7},$$

so 25 passes Miller's test for the base 7.

(6.3 # 8) Show that if a is an integer such that a is not divisible by 3 or such that a is divisible by 9, then $a^7 \equiv a \pmod{63}$.

By the corollary to Fermat's Little Theorem, $a^7 \equiv a \pmod{7}$. Suppose that $3 \nmid a$. Then $(a, 9) = 1$ and $\phi(9) = 6$, so by Euler's theorem, $a^6 \equiv a^{\phi(9)} \equiv 1 \pmod{9}$, so also $a^7 \equiv a \pmod{9}$. If $9 \mid a$ then $a \equiv 0 \pmod{9}$, so $a^7 \equiv a \equiv 0 \pmod{9}$. Therefore in either case, we have $a^7 \equiv a \pmod{7}$ and $a^7 \equiv a \pmod{9}$. Since $(7, 9) = 1$, then $a^7 \equiv a \pmod{63}$.

(6.3 # 10) Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$, if a and b are relatively prime positive integers.

First, $a^k \equiv 0 \pmod{a}$ and $b^k \equiv 0 \pmod{b}$ for any positive integer k. Then by Euler's Theorem,

$$a^{\phi(b)} + b^{\phi(a)} \equiv b^{\phi(a)} \equiv 1 \pmod{a},$$

and

$$a^{\phi(b)} + b^{\phi(a)} \equiv a^{\phi(b)} \equiv 1 \pmod{b}.$$

Then since $(a, b) = 1$, $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

(7.1# 8) Show that there is no positive integer n such that $\phi(n) = 14$.

Suppose n is a positive integer with $\phi(n) = 14$. We also know that if $n = p_1^{a_1} \cdots p_t^{a_t}$ then $\phi(n) = p_1^{a_1-1}(p_1 - 1) \cdots p_t^{a_t-1}(p_t - 1)$. So no prime $p > 15$ divides n, otherwise $\phi(n) > p - 1 > 14$. This leaves possible prime factors 2, 3, 5, 7, 11, and 13. But 5, 7, 11 and 13 can all be eliminated since 4, 6, 10, and 12 do not divide 14. But if $n = 2^a \cdot 3^b$ then $\phi(n) = 2^{a-1}(2-1) \cdot 3^{b-1}(3-1) = 2^a \cdot 3^{b-1}$, which is not divisible by 7. Therefore there is no n for which $\phi(n) = 14$.

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

Suppose that $m \mid n$, and write $n = p_1^{a_1} \cdots p_k^{a_k}$. Then $m = p_1^{b_1} \cdots p_k^{b_k}$ where $0 \le b_j \le a_j$ for all $1 \le j \le k$. Then

$$\frac{\phi(n)}{\phi(m)} = \frac{\prod_{j=1}^{k} p_j^{a_j-1}(p_j - 1)}{\prod_{j=1}^{k} p_j^{b_j-1}(p_j - 1)} = \prod_{j=1}^{k} p^{a_j - b_j}$$

is an integer, so $\phi(m) \mid \phi(n)$.

(7.2 # 4) For which positive integers n is the sum of divisors of n odd?

Let $n = p_1^{a_1} \cdots p_k^{a_k}$. Then $\sigma(n) = \prod_{j=1}^{k} \frac{p^{a_j+1}-1}{p-1}$. In order for $\sigma(n)$ to be odd, each term in this product must be odd. If $p = 2$, then $\frac{2^{a+1}-1}{2-1} = 2^a - 1$ is odd, for any positive integer a. If p is odd, then $\frac{p^{a+1}-1}{p-1} = 1 + p + p^2 + \cdots + p^a$. Since each power of p is odd, this sum is odd exactly when a is even. Therefore $\sigma(n)$ is odd if and only if the power of every odd prime dividing n is even.

(7.2 # 22) Give a formula for $\sigma_k(p^a)$, where p is prime and a is a positive integer.

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

(7.3 # 8) Show that any proper divisor of a deficient or perfect number is deficient.

Suppose that $a \mid n$ and $1 < a < n$. We want to prove that if $\sigma(n) \le 2n$, then $\sigma(a) < 2a$. We will prove the contrapositive, namely, if $\sigma(a) \ge 2a$, then $\sigma(n) > 2n$. There must be an integer k such that $ak = n$. Then if $c \mid a$, then $ck \mid ak = n$. Therefore

$$\sigma(n) = \sum_{d \mid n} d > \sum_{c \mid a} kc = k\sigma(a) \ge 2ka = 2n.$$

(7.3 # 20) Find all 3-perfect numbers of the form $n = 2^k \cdot 3 \cdot p$, where p is an odd prime.

First we note that $p \ne 3$, since then $n = 2^k \cdot 3^2$, so $13 = \sigma(3^2) \mid \sigma(n)$, and hence $\sigma(n) \ne 3n$. So we may assume $p \ne 3$. If $n = 2^k \cdot 3 \cdot p$ is 3-perfect, then $\sigma(n) = 3n = 2^k \cdot 3^2 \cdot p$, but also $\sigma(n) = \sigma(2^k)\sigma(3)\sigma(p) = (2^{k+1} - 1) \cdot 4(p - 1)$, so we set

$$2^k \cdot 3^2 \cdot p = (2^{k+1} - 1) \cdot 4(p - 1).$$

Since the right and left sides are equal, they must have the same prime power factorization, which is already given on the left. Then $k \geq 2$, so cancelling 4 from both sides, we have

$$2^{k-2} \cdot 3^2 \cdot p = (2^{k+1} - 1)(p - 1).$$

Now p and $p - 1$ are coprime, so p must divide $2^{k+1} - 1$. Similarly, $2^{k+1} - 1$ is odd, so 2^{k-2} must divide $p - 1$. Then there are integers m and r such that

$$2^{k-2} \cdot 3^2 \cdot p = (pm)(2^{k-2}r).$$

The only remaining factor on the left is 3^2, so there are three cases:

(a) $m = 9$ and $r = 1$,
(b) $m = r = 3$, and
(c) $m = 1$ and $r = 9$.

In case (a), we have $2^{k+1} - 1 = 9p$ and $p + 1 = 2^{k-2}$, so that $8(p + 1) = 2^{k+1}$. Substituting this into the first equation, we have $8(p + 1) - 1 = 9p$, and $p = 7$ is the only solution. Then $8 = 2^{k-2}$, so $k = 5$. So the only possible n in this case is $n = 2^5 \cdot 3 \cdot 7 = 672$. Using a similar argument for case (b), we get $p = 5$ and $k = 3$, so $n = 2^3 \cdot 3 \cdot 5 = 120$. Using this method for case (c) we conclude that $p = -1$. Since this is not possible, there are no solutions in this case. Therefore the only numbers of this form that are 3-perfect are 672 and 120.