P. Set 8 Solutions

1. a) Suppose that $d_1, d_2, \cdots, d_k$ are the divisors of m and $e_1, e_2, \cdots, e_l$ are the divisors of n. Then

$$\sigma(m) = d_1 + d_2 + \cdots + d_k$$
$$\sigma(n) = e_1 + e_2 + \cdots + e_l.$$

If these expressions are multiplied together and the product is expanded with the distributive property, the result is a sum of terms of the form $d_i \cdot e_j$, for $i = 1, 2, \cdots, k$ and $j = 1, 2, \cdots, l$.

We stated in class that each divisor of mn (when $\gcd(m,n)=1$) can be written uniquely as $d \cdot e$, where $d \mid m$ and $e \mid n$. Therefore these $k \cdot l$ products $d_i \cdot e_j$ are precisely the divisors of mn, with each divisor occurring exactly once. Hence

$$\sigma(m)\sigma(n) = (d_1 + \cdots + d_k) \cdot (e_1 + \cdots + e_l)$$
$$= d_1 e_1 + \cdots + d_i e_j + \cdots + d_k e_l$$
$$= \sigma(mn).$$

b) The divisors of p^e are $1, p, p^2, p^3, \cdots, p^e$. So

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e$$
$$= \boxed{\frac{p^{e+1} - 1}{p - 1}}$$

2. $\sigma(10) = \sigma(2)\sigma(5) = (1+2)(1+5) = 18.$

$\sigma(20) = \sigma(4)\sigma(5) = (1+2+4)(1+5) = 42.$

$\sigma(1728) = \sigma(2^6 \cdot 3^3) = \frac{2^7-1}{2-1} \cdot \frac{3^4-1}{3-1} = 127 \cdot 40 = 5080.$

$\sigma(4100) = \sigma(41 \cdot 2^2 \cdot 5^2) = 42 \cdot (1+2+4) \cdot (1+5+25) = 42 \cdot 7 \cdot 31 = 9114.$

3

a) Since $\gcd(2^k, m)=1$, it follows that $\sigma(n)=\sigma(2^k\cdot m)$ $=\sigma(2^k)\sigma(m) = (2^{k+1}-1)\cdot\sigma(m)$. This must equal $2n$, which is $2^{k+1}\cdot m$. Thus

$$(2^{k+1}-1)\,\sigma(m) = 2^{k+1}\cdot m.$$

Since $\gcd(2^{k+1}-1, 2^{k+1})=1$ and $2^{k+1} \mid (2^{k+1}-1)\sigma(m)$, it follows that $2^{k+1} \mid \sigma(m)$. Let $\ell = \sigma(m)/2^{k+1}$; it must be an integer.

Since $\dfrac{\sigma(m)}{2^{k+1}} = \dfrac{m}{2^{k+1}-1}$, these both equal ℓ, and thus

$$\sigma(m) = \ell\cdot 2^{k+1}$$
$$\& \qquad m = \ell\cdot(2^{k+1}-1).$$

b) The numbers $a\cdot(2^b-1)$, a, and 1 are all divisors of $a\cdot(2^b-1)$. Since $a\geq 2$ and $2^b-1\geq 2$, the inequalities

$$1 < a < a\cdot(2^b-1)$$

hold, so these are distinct divisors. So

$$\sigma(a(2^b-1)) \geq 1+a+a(2^b-1) = 1+a\cdot 2^b$$
$$\Rightarrow \sigma(a(2^b-1)) > a\cdot 2^b.$$

I needed $a\geq 2$ so that $a>1$; I needed $b\geq 2$ so that $a< a\cdot(2^b-1)$.

c) Let $a=\ell$ and $b=k+1$. Since $\sigma(a\cdot(2^b-1)) = a\cdot 2^b$ (by part a), the assumptions of part (b) cannot hold: either $a=1$ or $b=1$. But $b=k+1\geq 2$ since $k\geq 1$ (n is even). So $a=1$, i.e. $\underline{\ell=1}$.

4 a) $a^2 \equiv b^2 \bmod p \iff a^2 - b^2 \equiv 0 \bmod p$

$\iff (a+b)(a-b) \equiv 0 \bmod p$

$\iff p \mid (a+b)(a-b)$

$\iff p \mid (a+b)$ or $p \mid (a-b)$ (since p is prime)

$\iff a+b \equiv 0 \bmod p$ or $a-b \equiv 0 \bmod p$

$\iff a \equiv -b \bmod p$ or $a \equiv b \bmod p$.

b) $\lightning$ Suppose for contradiction that m is prime.

Since $a^2 \equiv b^2 \bmod m$, part (a) implies that either $a \equiv b \bmod m$ or $a \equiv -b \bmod m$. Since $|a-b| < m$, and $a \neq b$, it cannot be the case that $a \equiv b \bmod m$. So $a \equiv -b \bmod m$. Then $m \mid (a+b)$. But $2 \leq a+b \leq m$, so the only possibility is $a = b = \frac{1}{2}m$. But this is a contradiction, since $a \neq b$. $\lightning$

Therefore m cannot be prime; it is composite.

c) $150^2 = 22500 \equiv 169 \bmod 22331$.
so $150^2 \equiv 13^2 \bmod 22331$.

~~This means $150^2 - 13^2$ is divisible by 22331.~~ In fact,
~~it is equal to 22331. But~~
But $1 \leq 13 < 150 \leq \frac{1}{2} \cdot 22331$. By part (b), it follows that 22331 is composite.

Note: In fact, $22331 = 150^2 - 13^2 = (150+13)(150-13)$
$= 163 \cdot 137$.