Throughout this assignment, you may freely use the identity $(x-1)\sum_{i=0}^{n} x^i = x^{n+1}-1$, which holds for all $x \in \mathbb{R} \setminus \{0\}$ and $n \in \mathbb{N} \cup \{0\}$, which we proved in class.

Justify all answers!

(22 pts)

(1) [+8] Let $a, n \in \mathbb{N}$ with $n \geq 2$. Prove that if $a^n - 1$ is a prime, then $a = 2$ and n is a prime.

Proof. Using the identity mentioned above,

$$a^n - 1 = (a-1)\sum_{k=0}^{n-1} a^k.$$

Thus $(a-1) \mid (a^n - 1)$, so as $a^n - 1$ is prime, it must be the case that $a - 1 \in \{1, a^n - 1\}$. Now, as $a \in \mathbb{N}$ and $n \geq 2$, $a - 1 < a^n - 1$, so we must have $a - 1 = 1$. In other words, $a = 2$.

Now that we know $a = 2$, suppose for sake of contradiction that n is not prime. Thus, we can find $r, s \in \mathbb{N}$ with $1 < r, s < n$ and $n = rs$. Again appealing to the identity mentioned above

$$2^n - 1 = (2^r)^s - 1 = (2^r - 1)\sum_{k=0}^{r-1} 2^{rs},$$

so we have $(2^r - 1) \mid (2^n - 1)$. By assumption, $2^n - 1$ is prime, so $2^r - 1 \in \{1, 2^n - 1\}$. However, $r < n$, so $2^r - 1 = 1$. This implies that $r = 1$; a contradiction. Thus n must be a prime. $\square$

(2) For $n \in \mathbb{N}$, define

$$\sigma(n) := \sum_{d \mid n} d.$$

For example, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12$. We say that n is *perfect* if $\sigma(n) = 2n$. For example, 6 is perfect as $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

(a) [+2] Let p be a prime and $k \in \mathbb{N}$. Show that $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$.

Proof. As p is a prime, the only divisors of p^k are p^i for $i \in \{0, 1, \ldots, k\}$. Thus, by appealing to the identity mentioned above,

$$\sigma(p^k) = \sum_{i=0}^{k} p^i = \frac{p^{k+1}-1}{p-1}.$$ $\square$

(b) [+6] Let p be a prime and $n \in \mathbb{N}$ with $p \nmid n$. Prove that $\sigma(pn) = \sigma(p)\sigma(n)$.

Proof. As p is prime, the divisors of pn have the form d or pd for $d \mid n$. Further, as $p \nmid n$, these two types of divisors are distinct. Thus,

$$\sigma(pn) = \sum_{d \mid pn} d = \sum_{d \mid n} d + \sum_{d \mid n} pd = (1 + p)\sum_{d \mid n} d = \sigma(p)\sigma(n).$$ $\square$

(c) [+6] Let $n \in \mathbb{N}$ and suppose that $2^n - 1$ is prime. Show that $2^{n-1}(2^n - 1)$ is perfect.

Proof. As $2^n - 1$ is prime, we must have $n \geq 2$, so certainly $(2^n - 1) \nmid 2^{n-1}$ as $2^{n-1} < 2^n - 1$. Using parts (a) and (b) we calculate

$$\begin{aligned}\sigma\big(2^{n-1}(2^n - 1)\big) &= \sigma(2^{n-1})\sigma(2^n - 1) \\ &= \left(\frac{2^n - 1}{2 - 1}\right)\big(1 + (2^n - 1)\big) \\ &= (2^n - 1)2^n = 2\big(2^{n-1}(2^n - 1)\big).\end{aligned}$$

Thus, $2^{n-1}(2^n - 1)$ is perfect. □

(d) **Bonus.** [$+\infty$] Prove or disprove: There are no odd perfect numbers.

Proof. No effing clue. □

(3) **Bonus.** [+3] Let p_n be the nth prime, e.g. $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Prove that $p_n \leq 2^{2^{n-1}}$.[1]

Proof. As shown in class, if $N = (p_1 p_2 \cdots p_n) + 1$, then $p_i \nmid N$ for all $i \in [n]$. Thus, as there is some prime which must divide N, we know that, even if $p_{n+1} \nmid N$, we must have $p_{n+1} \leq N = (p_1 p_2 \cdots p_n) + 1$ for all $n \in \mathbb{N}$. We now prove the claim by induction on n.

Base case: For $n = 1$, $p_1 = 2 = 2^{2^{1-1}}$.

Induction hypothesis: For some $n_0 \in \mathbb{N}$, $p_m \leq 2^{2^{m-1}}$ for all $m \in \mathbb{N}$ and $m < n_0$.

Induction step: We must show that $p_{n_0} \leq 2^{2^{n_0-1}}$. By the earlier comment, we bound

$$\begin{aligned}p_{n_0} &\leq \big(p_1 \cdots p_{n_0-1}\big) + 1 \\ &\leq \prod_{i=1}^{n_0-1} 2^{2^{i-1}} + 1 && \text{(By the IH)} \\ &= 2^{\sum_{i=1}^{n_0-1} 2^{i-1}} + 1 \\ &= 2^{\sum_{i=0}^{n_0-2} 2^{i}} + 1 \\ &= 2^{2^{n_0-1}-1} + 1 && \text{(By the identity mentioned above)} \\ &\leq 2^{2^{n_0-1}}.\end{aligned}$$

Thus, by the principle of mathematical induction, the claim holds for all $n \in \mathbb{N}$. □

(Rewrite) [+3] Show that if n is not a prime, then $\sigma(n) \neq n + 1$.

Proof. If $n = 1$, then $\sigma(1) = 1 \neq 1+1$, so suppose $n \geq 2$ is not a prime. Thus, there is some $a \in \mathbb{N} \setminus \{1, n\}$ such that $a \mid n$. As such, $\sigma(n) \geq 1 + a + n > n + 1$, so $\sigma(n) \neq n + 1$. □

---

[1] In fact, it can be shown through a similar idea that $p_n \leq 2^n$, but we have not developed all of the tools to do this. Through much more complicated techniques, it can actually be shown that $p_n = \big(1 + c(n)\big)n \log n$ where $c(n) \to 0$ as $n \to \infty$.