1) [14 points] Prove that if $(a, b) = 1$, then $(a - b, a + b)$ is either 1 or 2.

Solution. Let $d = ((a - b), (a + b))$. Hence $d \mid (a - b)$ and $d \mid (a + b)$. So, by our old lemma, we have that $d \mid ((a-b)+(a+b)) = 2a$. Also, $d \mid ((a+b)-(a-b)) = 2b$. So, d is a common divisor of $2a$ and $2b$.
By properties of the GCD we know that $d \mid (2a, 2b)$. By a HW problem [1.62] we know that $(2a, 2b) = 2(a, b) = 2$, and hence $d \mid 2$, so $d = 1$ or $d = 2$. □

2) [14 points] Remember that

$$(x^n - y^n) = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + x^2y^{n-3} + xy^{n-2} + y^{n-1}).$$

Prove that if $a^n - 1$ is prime for some $a, n \in \mathbb{Z}_{>1}$, then $a = 2$ and n is itself prime.
[**Hint:** First, prove that $a = 2$. For the second part, assume that $n = r \cdot s$, with $r, s > 1$, to derive a contradiction. Note that $2^n = 2^{rs} = (2^r)^s$.]

Proof. We have

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Since $n \geq 2$, the second factor is at least $a + 1 > 1$. If $a > 2$, then also $(a - 1) > 1$ and the number would be composite. So, we must have that $a = 2$.
Now, assume $n = r \cdot s$, with $r, s > 1$. Then,

$$(2^n - 1) = (2^{rs} - 1) = ((2^r)^s - 1) = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 2^r + 1).$$

Since $r > 1$, we have that $2^r - 1 > 1$ and since $s > 1$ we have that $((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 2^r + 1) > 1$. Hence, $2^n - 1$ is composite, a contradiction.

□