

### Problems to think about solution (Chapter 4)

1. Prove that if  $p$  is a prime number that satisfies  $p \equiv 1 \pmod{4}$  then whenever  $g$  is primitive mod  $p$ , so is  $-g$ .
2. Prove that if  $p$  and  $2p + 1$  are prime numbers with  $p \equiv 3 \pmod{4}$  then  $-2$  is primitive mod  $2p + 1$ .
3. Prove that if  $p$  and  $p' = 2^k p + 1$  are odd primes then  $a$  is a primitive root mod  $p'$  if and only if  $a^{2^k} \not\equiv 1 \pmod{p'}$  and  $\left(\frac{a}{p'}\right) = -1$ .
4. Identify all Fermat and Mersenne primes  $p$  that have 2 as a primitive root.