

**book problems**

§9.1 #7 If  $p = 2^k + 1$  is prime, verify that every quadratic nonresidue of  $p$  is a primitive root of  $p$ . Let  $a$  be a quadratic nonresidue of  $p$ . Then by Euler's Criterion,  $a^{(p-1)/2} \equiv -1 \pmod{p}$ . Since  $p$  is a prime,  $\phi(p) = p - 1 = 2^k$ . Therefore Euler's Criterion says  $a^{2^{k-1}} \equiv -1 \pmod{p}$ . Squaring both sides of this relation we see that  $a^{2^k} \equiv 1 \pmod{p}$ . Let  $h$  be the order of  $a \pmod{p}$ . Then  $h \mid 2^k$  and we can write  $h = 2^r$  for some  $1 \leq r \leq k$ . If  $r \leq k - 1$  then we have

$$(a^h)^{2^{k-1-r}} \equiv 1^{2^{k-1-r}} \equiv 1 \pmod{p}$$

and

$$(a^h)^{2^{k-1-r}} = (a^{2^r})^{2^{k-1-r}} = 2^{k-1} \equiv -1 \pmod{p}.$$

This implies that  $1 \equiv -1 \pmod{p}$  or  $p \mid 2$ . This is a contradiction since  $p$  is an odd prime. Therefore  $r \geq k$  and by what we've shown above, this implies that  $r = k$ . Therefore the order of  $a$  is  $2^k = \phi(p)$  and hence  $a$  is a primitive root of  $p$ .