Math 255 - Spring 2017
Homework 10 Solutions

1. First, if $k = 0$ then $p = 2$ and there are no quadratic nonresidues modulo 2. Therefore the statement is vacuously true. Therefore we may assume $p > 2$.

   Let $p = 2^k + 1$ and a be such that $\left(\frac{a}{p}\right) = -1$. Then by Euler's criterion we have

$$\begin{aligned} -1 &= \left(\frac{a}{p}\right) \\ &\equiv a^{(p-1)/2} \pmod{p} \\ &\equiv a^{2^k/2} \pmod{p} \\ &\equiv a^{2^{k-1}} \pmod{p}, \end{aligned}$$

   where we have used that $p = 2^k + 1$ for the second congruence.

   We must show that a has order $\varphi(p) = p-1 = 2^k$. First we show that $a^{2^k} \equiv 1 \pmod{p}$. Indeed:

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

   Second, we must show that there is no ℓ with $0 < \ell < p - 1 = 2^k$ such that $a^\ell \equiv 1 \pmod{p}$, so that 2^k is the least positive integer with $a^{2^k} \equiv 1 \pmod{p}$. To do this, we suppose by way of a contradiction that a has order ℓ modulo p, and $0 < \ell < 2^k$. By Theorem 8.1, we must have that ℓ divides $\varphi(p) = 2^k$. Since 2^k is a power of a prime, all of its divisors are of the form 2^j for $0 \le j \le k$. Therefore $\ell = 2^j$ for some $0 \le j < k$ (the strict inequality is because we assume $\ell = 2^j < 2^k$). If a has order $\ell = 2^j$, we have that

$$a^\ell = a^{2^j} \equiv 1 \pmod{p}.$$

   Now to obtain the contradiction, it suffices to raise both sides of this equation to the power 2^{k-j-1}, noting that $k - j - 1 \ge 0$ since $j < k$. On the left hand side we obtain

$$(a^\ell)^{2^{k-j-1}} = (a^{2^j})^{2^{k-j-1}} = a^{2^j \cdot 2^{k-j-1}} = a^{2^{k-1}},$$

   and on the right hand side we get

$$1^{2^{k-j-1}} = 1.$$

   Therefore, if $a^{2^j} \equiv 1 \pmod{p}$ with $0 < j < k$, it follows that

$$a^{2^{k-1}} \equiv 1 \pmod{p},$$

   which is a contradiction to Euler's criterion, since $p > 2$ so $-1 \not\equiv 1 \pmod{p}$.

2. (a) Here $a = 8$ and $p = 11$, so $\frac{p-1}{2} = 5$. The set S from Gauss's Lemma is

$$S = \{8, 16, 24, 32, 40\}.$$

We compute the remainder of each of these integers when we divide by 11:

$$S_{remainders} = \{8, 5, 2, 10, 7\}.$$

Then in the notation of the theorem, n is the number of elements of $S_{remainders}$ that are greater than $\frac{p}{2} = \frac{11}{2} = 5.5$. There are three such numbers (7, 8 and 10). Therefore

$$\left(\frac{8}{11}\right) = (-1)^3 = -1.$$

Note on the proof of Gauss's Lemma: In the notation of the proof, we have $r_1 = 2$, $r_2 = 5$ (the small remainders) and $s_1 = 7$, $s_2 = 8$ and $s_3 = 10$ (the big remainders). If we look at the list $r_1, r_2, p-s_1, p-s_2, p-s_3$, this is the list of integers $2, 5, 4, 3, 1$, and indeed we have each integer between 1 and $\frac{p-1}{2} = 5$, exactly once. The congruence that proves the theorem is

$$\begin{aligned}
5! &= 2 \cdot 5 \cdot 4 \cdot 3 \cdot 1 \\
&= 2 \cdot 5 \cdot (11-7) \cdot (11-8) \cdot (11-10) \\
&\equiv 2 \cdot 5 \cdot (-7) \cdot (-8) \cdot (-10) \pmod{11} \\
&= (-1)^3\, 2 \cdot 5 \cdot 7 \cdot 8 \cdot 10 \\
&\equiv (-1)^3\, 24 \cdot 16 \cdot 40 \cdot 8 \cdot 32 \pmod{11} \\
&= (-1)^3\, (3 \cdot 8)(2 \cdot 8)(5 \cdot 8)(1 \cdot 8)(4 \cdot 8) \\
&= (-1)^3\, 8^5\, 5!
\end{aligned}$$

Canceling $5! = 120 \equiv 10 \pmod{11}$ from both sides (we can do this because it is a unit), we get

$$1 \equiv (-1)^3\, 8^5 \pmod{11}$$

or

$$8^5 \equiv (-1)^3 \pmod{11},$$

and $8^5 \equiv \left(\frac{8}{11}\right) \pmod{11}$ by Euler's Criterion.

(b) Here $a = 7$ and $p = 13$, so $\frac{p-1}{2} = 6$. The set S from Gauss's Lemma is

$$S = \{7, 14, 21, 28, 35, 42\}.$$

We compute the remainder of each of these integers when we divide by 13:

$$S_{remainders} = \{7, 1, 8, 2, 9, 3\}.$$

Then in the notation of the theorem, n is the number of elements of $S_{remainders}$ that are greater than $\frac{p}{2} = \frac{13}{2} = 6.5$. There are three such numbers (7, 8 and 9). Therefore

$$\left(\frac{7}{13}\right) = (-1)^3 = -1.$$

3. Note that for this statement to be correct we must assume $n \geq 1$. (If $n = 0$, then $p = 2$ and $\left(\frac{3}{2}\right) = \left(\frac{1}{2}\right) = 1$.)

   We use Quadratic Reciprocity since both 3 and p are odd primes. First, we check if $\left(\frac{3}{p}\right)$ and $\left(\frac{p}{3}\right)$ have the same or opposite signs:

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}} = (-1)^{\frac{2^{2n}}{2}} = (-1)^{2^{2n-1}} = 1,$$

   since 2^{2n-1} is even. So they have the same sign and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$.

   Now it is a matter of deciding if p is a square modulo 3 or not. Thankfully, there are only two choices for p modulo 3: Either $p \equiv 1 \pmod 3$, in which case it is a square, or $p \equiv 2 \pmod 3$, in which case it is not a square. (We get that 2 is not a square modulo 3 by computing all the square: $1^2 \equiv 1 \pmod 3$ and $2^2 \equiv 1 \pmod 3$.) We have

$$\begin{aligned} p = 2^{2n} + 1 &= (2^2)^n + 1 \\ &= 4^n + 1 \\ &\equiv 1^n + 1 \pmod 3 \\ &\equiv 1 + 1 = 2 \pmod 3. \end{aligned}$$

   Therefore any prime p with $p = 2^{2n} + 1$ is congruent to 2 modulo 3 and therefore not a square modulo 3. We conclude that

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1.$$

Answer to bonus question: If $k = 1$, then $p = 3$ is a prime. Suppose now that k is odd, we will show that $2^k + 1$ cannot be a prime. Indeed, in that case, if $k = 2n + 1$, say, we have

$$\begin{aligned} 2^k + 1 &= 2^{2n+1} + 1 \\ &= 2 \cdot 2^{2n} + 1 \\ &= 2 \cdot 4^n + 1 \\ &\equiv 2 \cdot 1^n + 1 \pmod 3 \\ &= 2 + 1 \equiv 0 \pmod 3. \end{aligned}$$

In other words, if k is odd then $2^k + 1$ is divisible by 3, and therefore cannot be a prime except if it is equal to 3.

In problem 1, there is no restriction on k because the result applies when $p = 3$ as well (2 is the only quadratic nonresidue, and it is a primitive root of 3). In problem 3, there is a restriction on k ($k = 2n$ is even) because the result does not apply when $p = 3$ (the Legendre symbol becomes $\left(\frac{3}{3}\right)$, which is 0, not -1).