Math 567, Assignment #9: Solutions

1. First method: We compute 5^{11} modulo 23. We successively compute $5^2 \equiv 25 \equiv 2$, $5^4 \equiv (5^2)^2 \equiv 2^2 \equiv 4$, and $5^8 \equiv (5^4)^2 \equiv 4^2 \equiv 16$, so $5^{11} \equiv 5^{8+2+1} \equiv 5^8\, 5^2\, 5^1 \equiv 16 \cdot 2 \cdot 5 \equiv 160 \equiv -1 \pmod{23}$, so 5 is not a quadratic residue mod 23.

Second method: Writing the eleven numbers 5,10,15,20,25,30,35,40,45,50, 55 in terms of the balanced complete system of residues mod 23, we get 5,10, -8,-3,2,7,-11,-6,-1,4,9. Since five of these numbers have minus signs, $\left(\frac{5}{23}\right) = (-1)^5 = -1$, whence 5 is not a quadratic residue mod 23.

Third method: Set $p = 5$, $q = 23$, and $q' = 3$. Since $23 \equiv 3 \pmod{4 \cdot 5}$, we have $\left(\frac{5}{23}\right) = \left(\frac{5}{3}\right)$. Furthermore, $\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)$ (since $5 \equiv 2 \pmod 3$), and we already know that 2 is not a quadratic residue mod 3 (or can easily check this if we've forgotten). Hence $\left(\frac{5}{23}\right) = \left(\frac{2}{3}\right) = -1$, so 5 is not a quadratic residue mod 23.

2. If we square $a^{(p+1)/4}$ (or its negative), we get $a^{(p+1)/2}$. We wish to show that this is just $a \pmod p$.

Method 1: Since a is a quadratic residue, we can write $a \equiv b^2 \pmod p$, with p not dividing b. Then $a^{(p+1)/2} \equiv (b^2)^{(p+1)/2} \equiv b^{p+1} \equiv b^{p-1}b^2 \equiv 1 \cdot a \equiv a \pmod p$, where the intermediate step b^{p-1} is a consequence of Fermat's little theorem. (Note that the logic here is valid but funny: to show that $a^{(p+1)/4}$ is a solution of $x^2 \equiv a \pmod p$, we make use of the fact that at least one solution exists!)

Method 2: Let r be a primitive root mod p. We know that we can write a as $r^{2i} \pmod p$, since a is a quadratic residue (see the Corollary to Theorem 9.4). Then $a^{(p+1)/2} \equiv (r^{2i})^{(p+1)/2} \equiv r^{i(p+1)} \equiv (r^i)^p r^i \equiv r^i \cdot r^i \equiv r^{2i} \equiv a \pmod p$, where again we are using Fermat's little theorem.

Method 3: To show that $a^{(p+1)/2}$ is congruent to a, let us first prove that its square is congruent to a^2: $(a^{(p+1)/2})^2 \equiv a^{p+1} \equiv a^p \cdot a \equiv a \cdot a \equiv a^2 \pmod p$. Since a^2 has only two square roots mod p, namely $\pm a$, it follows that $a^{(p+1)/2}$ is either a or $-a$. Recall, however, that when $p \equiv 3 \pmod 4$ as is the case here, $\left(\frac{-1}{4}\right) = -1$; since a is a quadratic residue, $-a$ must be a quadratic nonresidue (use $\left(\frac{-a}{p}\right) = \left(\frac{(-1)(a)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = -\left(\frac{a}{p}\right)$). If we had $a^{(p+1)/2} \equiv -a \pmod p$, then we would have $(a^{(p+1)/4})^2 \equiv -a \pmod p$, so that $-a$ would be a quadratic residue mod p after all: contradiction! Hence $a^{(p+1)/2} \equiv +a \pmod p$, as desired.

In any case, we have found two solutions to the congruence $x^2 \equiv a \pmod p$, and since a polynomial congruence of degree 2 has at most 2 roots, we have found all the solutions.

(Note: If we were to try to apply the formula $x \equiv \pm a^{(p+1)/4}$ when a is a quadratic nonresidue mod p, we would get a solution of the congruence $x^2 \equiv -a \pmod p$.)

3. By Theorem 9.2 (part (d)) and the Corollary to Theorem 9.2, we have $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = (+1)(+1) = +1$. Also, $(p-1)/4$ times 4 is $p-1$, so $\left(\frac{(p-1)/4}{p}\right)$ times $\left(\frac{4}{p}\right)$ is $\left(\frac{p-1}{p}\right)$; since $\left(\frac{4}{p}\right) = +1$ and $\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = +1$, $\left(\frac{(p-1)/4}{p}\right) = \left(\frac{(p-1)}{p}\right) / \left(\frac{4}{p}\right) = (+1)/(+1) = +1$.

4. We apply Euler's criterion: if a is a quadratic nonresidue mod p, p must be odd, and we must have $a^{(p-1)/2} \equiv -1 \not\equiv 1 \pmod p$. Let $k = \mathrm{ord}_p\, a$. We know that k divides $p-1$. Note, however, that when $p-1$ is a power of 2, every divisor d of $p-1$ other than $p-1$ itself is a divisor of $(p-1)/2$. Since $a^{(p-1)/2} \not\equiv 1$, we have $a^d \not\equiv 1$ for every divisor d of $(p-1)/2$, so k cannot equal any such divisor. Hence k must equal $p-1$, and a must be a primitive root.

5. For all i, $b + ip \equiv b \pmod p$, so $(b+ip)^2 \equiv b^2 \equiv a \pmod p$. Now, every number that is congruent to $a \pmod p$ must be congruent to a or $a+p$ or $a+2p$ or ... or $a + (p-1)p \pmod{p^2}$. (Proof: Suppose $x \equiv a \pmod p$. Then $\frac{x-a}{p}$ is an integer, and must satisfy $\frac{x-a}{p} \equiv j \pmod p$ for some j; hence p divides $\frac{x-a}{p} - j$, whence p^2 divides $(x-a) - jp = x - (a+jp)$, so that $x \equiv a + jp \pmod{p^2}$.) Thus, for every i in $0, 1, \ldots, p-1$ there exists j in $0, 1, \ldots, p-1$ such that $(b+ip)^2 \equiv a + jp \pmod{p^2}$. Must there exist an i that gives $j = 0$? This will follow if we can show that distinct values of i give rise to distinct values of j (because every injective function from the finite set $\{0, 1, 2, \ldots, p-1\}$ to itself must also be surjective; i.e., "one-to-one" implies "onto"). So, we must show that if i, i' are not congruent mod p, then $(b+ip)^2$ and $(b+i'p)^2$ are not congruent mod p^2.

Since $(b+ip)^2 \equiv b^2 + 2ibp$ and $(b+i'p)^2 \equiv b^2 + 2i'bp$, this is tantamount to showing that $2ibp \not\equiv 2i'bp \pmod{p^2}$. That is, we wish to show that p^2 does not divide $2ibp - 2i'bp = 2(i-i')bp$, which is equivalent to showing that p does not divide $2(i-i')b$. But if i, i' are non-congruent mod p, neither 2 nor $i - i'$ is a multiple of p, and $b^2 \equiv a \not\equiv 0 \pmod p$ implies that b is not a multiple of p either. Hence $2(i-i')$ is not a multiple of p, which proves the claim.

The above proof is non-constructive. There is an alternative way of actually finding the i-value that gives $j=0$: that is, we can solve $(b+ip)^2 \equiv a \pmod{p^2}$ for i. Rewrite this congruence successively:

$$\begin{aligned}
(b+ip)^2 &\equiv a \ (\mathrm{mod} p^2) \\
b^2+2ibp+p^2 &\equiv a \ (\mathrm{mod} p^2) \\
b^2+2ibp &\equiv a \ (\mathrm{mod} p^2) \\
2ibp &\equiv a-b^2 \ (\mathrm{mod} p^2) \\
2ib &\equiv \frac{a-b^2}{p} \ (\mathrm{mod} p) \\
i &\equiv \frac{a-b^2}{p} \cdot (2b)' \ (\mathrm{mod} p)
\end{aligned}$$

where $(2b)'$ denotes the multiplicative inverse of $2b$ modulo p. It can be checked that all steps in this chain are reversible, so the i given by this formula does the job.

In fact, it can be shown that if $x^2 \equiv a \pmod{p}$ has a solution, then so do $x^2 \equiv a \pmod{p^2}$ and $x^2 \equiv a \pmod{p^3}$ and so on ad infinitum. This works whenever p is an odd prime. If p is 2, the claim does not hold: $x^2 \equiv 3$ has a solution mod 2 but not mod 2^2, and $x^2 \equiv 5$ has a solution mod 2 and mod 2^2 but not mod 2^3. However, there is still a version of the claim that applies to powers of 2: if $x^2 \equiv a$ has a solution mod 8, then it has a solution mod 16, mod 32, etc.

6. We can write the congruence as $(2x-1)(3x-1) \equiv 0 \pmod{n}$. Let us first proof that the claim is true when n is a prime power p^k $(k>0)$. If $p \neq 2$, then $\gcd(2,p^k)=1$, so 2 has a multiplicative inverse modulo p^k; if we call this inverse a, then we have $2a \equiv 1 \pmod{p^k}$, so $2a-1 \equiv 0 \pmod{p^k}$ and $(2a-1)(3a-1) \equiv 0 \pmod{p^k}$. Similarly, if $p \neq 3$, then $\gcd(3,p^k)=1$, so 3 has a multiplicative inverse modulo p^k; if we call this inverse a, then we have $3a \equiv 1 \pmod{p^k}$, so $3a-1 \equiv 0 \pmod{p^k}$ and $(2a-1)(3a-1) \equiv 0 \pmod{p^k}$. In either case, the congruence $(2x-1)(3x-1) \equiv 0$ has a solution mod p^k.

Now drop the assumption that n is a prime power, and write n as a product of one or more prime powers: $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. By the result proved in the preceding paragraph, there exist $a_1, a_2, \ldots, a_r$ such that

$$(2a_i - 1)(3a_i - 1) \equiv 0 \pmod{p_i^{k_i}}$$

for $i = 1, 2, \ldots, r$. By the Chinese Remainder Theorem, there exists x such that $x \equiv a_i \pmod{p_i^{k_i}}$ for $i = 1, 2, \ldots, r$, and it is easy to check that this x must satisfy $(2x-1)(3x-1) \equiv 0 \pmod{n}$. Indeed, for each i, we have $x \equiv a_i \pmod{p_i^{k_i}}$, implying $(2x - 1)(3x - 1) \equiv (2a_i - 1)(3a_i - 1) \equiv 0 \pmod{p_i^{k_i}}$. Since $(2x - 1)(3x - 1)$ is a multiple of all of the relatively prime numbers $p_1^{k_1}, \ldots, p_r^{k_r}$, it must also be a multiple of their product, which is n.