McGill University
Math 346B/377B: Number Theory

Assignment 4 Solutions

1. (p.97,#10) We have $a \equiv \sigma_{p-2} \equiv 0 \pmod{p}$ for $p \geq 5$.

2. (p.107,#18) If g, h primitive roots mod p we have
$$(gh)^{(p-1)/2} = g^{(p-1)/2} g^{(p-1)/2} \equiv (-1)(-1) = 1 \pmod{p}.$$

3. (p.107,#20) Since $\phi(101) = 100$, $2^{20} \equiv 95 \pmod{101}$ and $2^{50} \equiv -1 \pmod{101}$ we see that a is a primitive root mod 101. If $f(x) = x^{101} - 1$, we have $f(2) \equiv 9292 \pmod{101^2}$ and $f'(2) \equiv 99 \pmod{101}$ so that, by Hensel's Lemma, $2 - (9292)(99) \equiv 8385 \pmod{101^2}$ is the unique lifting of 2 to a root of $f(x)$ mod 101^2. Any other lifting of 2 to $\mathbb{Z}/101\mathbb{Z}$ must have order larger than and divisible by 101 and also divide 100(101) so that the order must be 100(101) since 101 is prime.

4. (p.140,#6) We have $(\frac{150}{1009}) = (\frac{2}{1009})(\frac{3}{1009})(\frac{25}{1009}) = (\frac{3}{1009}) = (\frac{1009}{3}) = (\frac{1}{3}) = 1$ so that 150 is a square mod the prime 1009.

5. (p.141,#8) We have $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p}) = (\frac{2}{p})(\frac{p}{5})$ and $(\frac{2}{p}) = 1$ iff $p \equiv \pm 1 \pmod{8}$ with $(\frac{p}{5}) = 1$ iff $p \equiv \pm 1 \pmod{5}$. By the CRT it follows that $(\frac{10}{p}) = 1$ iff $p \equiv \pm 1, \pm 9, \pm 3, \pm 13 \pmod{40}$.

6. (p.141,#9) We have $(\frac{5}{q}) = (\frac{q}{5})$ which is equal to 1 iff $q \equiv \pm 2 \pmod{5}$.

7. (p.147,#5) Since 1013 is a prime we have $x^4 \equiv 25 \pmod{1013}$ iff $x^2 \equiv \pm 5 \pmod{1013}$. The latter congruences have no solution since $(\frac{-5}{1013}) = (\frac{5}{1013}) = (\frac{1013}{5}) = (\frac{3}{5}) = -1$.

8. (p.141,#13) Since $(\frac{-3}{p}) = (\frac{p}{3})$, we see that every prime divisor $p \neq 2, 3$ of $n^2 + 3$ is congruent to 1 mod 3. If $p_1, p_2, \ldots, p_k$ are primes of the form $3m + 1$ it follows that any prime divisor of $(p_1 p_2 \cdots p_k)^2 + 1$ will be a new prime of the form $3n + 1$.

9. (p.141,#15) Since $q - 1$ is a power of 2 any quadratic nonresidue mod q is a primitive root mod q if q is prime. If $3^{(q-1)/2} \equiv -1 \pmod{q}$ then 3 must be of order $q - 1$ which implies that q is prime.

10. (p.141,#16) It suffices to show that $3, 5, 7$ are quadratic nonresidues mod p under the given conditions. We have $(\frac{-q}{p}) = (\frac{p}{q})$ which is -1 iff p is not a quadratic residue mod q. Now $p \equiv 2 \pmod{3}$ and $p \equiv 2 \pmod{5}$ if $n \geq 2$. Finally, $p \equiv 3$ or $5 \pmod{7}$ if $n \geq 2$.