18.781 Solutions to Problem Set 5

1. Note that $41 - 1 = 2^3 \cdot 5$. Start with a quadratic nonresidue mod 41, say, 3. Now $b = 3^5 = 81 \cdot 3 \equiv -3 \pmod{41}$, which has order exactly 8. $(-3)^{-1} \equiv -14 \pmod{41}$.

Now we calculate a square root of 21. First, check that 21 is a square:

$$21^{(41-1)/2} = 21^{20} = 3^{20} \cdot 7^{20} \equiv -1 \cdot 7^{20}$$
$$\equiv -1 \cdot 49^{10} \equiv -1 \cdot 3^{10} \equiv -2^{30}$$
$$\equiv -2^{20} \cdot 2^{10} \equiv -1 \cdot 1024$$
$$\equiv 1 \pmod{41}.$$ 

Next, calculate

$$21^{10} \equiv 441^5 \equiv (-10)^5 \equiv 18 \cdot 18 \cdot (-10)$$
$$\equiv 324 \cdot (-10) \equiv (-8)(-10)$$
$$\equiv -1 \pmod{41}.$$ 

So update

$$A = (21)/(-3)^2 \equiv 21 \cdot 14^2$$
$$= 21 \cdot 196 \equiv 21 \cdot (-9)$$
$$\equiv 16 \pmod{41}.$$ 

Next, since $16^5 \equiv 2^{20} \equiv 1 \pmod{41}$, there is no need to modify $A$ and $b$ for this step. We’re at the stage where $A^{\text{odd}} \equiv 1 \pmod{41}$, so a square root of $A$ is $A^{(5+1)/2} = 16^3 \equiv -4 \pmod{41}$. (Note: we could have guessed a square root of 16 anyway since it’s a perfect square.) Thus, a square root of 21 is given by $(-3)(-4) \equiv 12 \pmod{41}$. Check: $12^2 = 144 \equiv 21 \pmod{41}$. The other square root of 21 mod 41 is -12.

2. First, observe that $(2p - 1)/3$ is an integer, and that by Fermat’s Little Theorem

$$\left(a^{(2p-1)/3}\right)^3 = a^{2p-1}$$
$$= a(a^{p-1})^2$$
$$\equiv a \pmod{p}.$$ 

Since 3 and $p - 1$ are coprime, this is the unique cube root of $a$.

3. (a) Since $p \nmid a$, we complete the square:

$$ax^2 + bx + c = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right)$$
$$= a\left(\left(x + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2}\right)$$
$$= a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{(b^2 - 4ac)}{4a^2}\right]$$
$$= \frac{1}{4a}[2ax + b)^2 - (b^2 - 4ac)].$$
Letting $y = 2ax + b$, the congruence $f(x) \equiv 0 \pmod{p}$ is equivalent to $y^2 \equiv D \pmod{p}$. If $p | D$ then obviously $y \equiv 0$ is the only solution, and thus $x \equiv -b/2a$. Else, if $p \nmid D$, then there are either 0 or 2 solutions depending on whether $D$ is or is not a square mod $p$. Finally, $f'(x_0) = 2ax_0 + b = y_0$ must be nonzero mod $p$ because its square $D$ is nonzero.

(b) By part (a), $x^2 \equiv a \pmod{p}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions mod $p$. Since $f(x) = x^2 - a$ satisfies the criterion of Hensel’s Lemma, every solution mod $p$ lifts to a unique solution mod $p^e$. Hence, the number of solutions mod $p^e$ is $1 + \left(\frac{a}{p}\right)$ as well.

4. We use the Chinese Remainder Theorem to decompose each congruence into a system of congruences with factors of the modulus.

(a) We have $118 = 2 \cdot 59$. Now the congruence $x^2 \equiv -2 \equiv 0 \pmod{2}$ has a unique solution, and $x^2 \equiv -2 \pmod{59}$ has two solutions because

$$\left(\frac{-2}{59}\right) = \left(\frac{-1}{59}\right) \left(\frac{2}{59}\right) = (-1) \cdot (-1) = 1.$$ 

Therefore there are two solutions to the original congruence.

(b) The congruence $x^2 \equiv -1 \pmod{4}$ has no solutions, so there are no solutions.

(c) We have $365 = 5 \cdot 73$. There are two solutions to each of the congruences $x^2 \equiv -1 \pmod{5}$ and $x^2 \equiv -1 \pmod{73}$, so there are $2 \cdot 2 = 4$ solutions.

(d) Since $227$ is prime, we use quadratic reciprocity:

$$\left(\frac{7}{227}\right) = -\left(\frac{227}{7}\right) = -\left(\frac{3}{7}\right) = -(1) = 1.$$ 

So there are two solutions.

(e) We have $789 = 3 \cdot 263$. The first congruence, $x^2 \equiv 267 \equiv 0 \pmod{3}$, has exactly one solution. The second, $x^2 \equiv 267 \equiv 4 \pmod{263}$, has two solutions. Thus there are two solutions.

5. Assume $p$ is odd, since if $p = 2$ this is obvious. If we let $x = g^k$, where $g$ is a primitive root mod $p$, then we have $g^{4k} \equiv 16 \pmod{p}$. This equation has a solution if and only if

$$1 \equiv 16^{\frac{p-1}{\gcd(8,p-1)}}$$

$$= 2^{4(p-1)/\gcd(8,p-1)} \pmod{p}.$$ 

Now if $8 \nmid p - 1$, then $\gcd(8,p-1)$ is 2 or 4. It follows that $4(p-1)/\gcd(8,p-1)$ is a multiple of $p - 1$, so $2^{4(p-1)/\gcd(8,p-1)} \equiv 1 \pmod{p}$ by Fermat.

On the other hand, if $8 | p - 1$, then 2 is a quadratic residue mod $p$, and thus $2^{4(p-1)/\gcd(8,p-1)} = 2^{(p-1)/2} \equiv 1 \pmod{p}$.

6. We will argue by contradiction, as in Euclid’s proof. Suppose there are only finitely many such primes, say, $p_1, \ldots, p_n$. Let

$$N = (p_1 \cdots p_n)^2 - 2.$$ 

First, note that $N$ is odd because the $p_i$ are all odd. Also, since $p_1 = 7$, we have $N \geq 7^2 - 2 > 1$.

Finally, since $p_i \equiv 1 \pmod{8}$, $N \equiv 1 - 2 \equiv 7 \pmod{8}$.

Now $N$ is divisible only by odd primes, and if $p$ is a prime dividing $N$ then $(p_1 \cdots p_n)^2 \equiv 2 \pmod{p}$, so $\left(\frac{2}{p}\right) = 1$. Thus $p \equiv \pm 1 \pmod{8}$. But not all the primes dividing $N$ can be congruent to 1 mod 8, as that would force $N \equiv 1 \pmod{8}$, so there exists some prime $p | N$ congruent to 7 mod 8. However, $p$ cannot be one of the $p_i$, because

$$(p_i, N) = (p_i, (p_1 \cdots p_n)^2 - 2) = (p_i, 2) = 1.$$ 

Contradiction.
7. Obviously we need \( p \neq 2, 5 \). Then, by quadratic reciprocity,

\[
\left( \frac{10}{p} \right) = \left( \frac{2}{p} \right) \left( \frac{5}{p} \right) = \left( \frac{2}{p} \right) \left( \frac{p}{5} \right).
\]

We have

\[
\left( \frac{2}{p} \right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}
\]

and

\[
\left( \frac{5}{p} \right) = \begin{cases} +1 & \text{if } p \equiv \pm 3 \pmod{8} \\ -1 & \text{if } p \equiv \pm 2 \pmod{5} \end{cases}
\]

So the product will depend on \( p \mod 40 \). By direct calculation,

\[
\left( \frac{2}{p} \right) \left( \frac{p}{5} \right) = \begin{cases} +1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40} \\ -1 & \text{if } p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40} \end{cases}
\]

8. (a) Clearly we need \( p \neq 3 \), and everything is a square mod 2, so let’s restrict our attention to primes greater than 3. Then, by quadratic reciprocity,

\[
\left( \frac{-3}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{3}{p} \right)
\]

\[
= (-1)^{\frac{p-1}{2}} (-1)^{\frac{3-1}{2}} \left( \frac{p}{3} \right)
\]

\[
= \left( \frac{p}{3} \right)
\]

\[
= \begin{cases} +1 & \text{if } p \equiv 1 \pmod{3} \\ -1 & \text{if } p \equiv -1 \pmod{3} \end{cases}
\]

So \(-3\) is a quadratic residue mod \( p \) if and only if \( p = 2 \) or \( p \equiv 1 \pmod{3} \).

(b) For primes of the form \( 3k - 1 \): Suppose there are finitely many, say, \( p_1, p_2, \ldots, p_n \) with \( p_1 = 2 \). Then we let \( N = 3p_1 \cdots p_n - 1 \) and argue as in Euclid’s proof. Since \( N \equiv -1 \pmod{3} \) and \( N \) is odd, \( N \) must be divisible by some odd prime equivalent to \(-1 \pmod{3}\).

For primes of the form \( 3k + 1 \): Now we use \( N = (2p_1 \cdots p_n)^2 + 3 \). Then \( N \) is odd, and if \( p|N \), then \(-3 \equiv (2p_1 \cdots p_n)^2 \pmod{p} \) so \(-3\) is a quadratic residue mod \( p \). This implies that \( p \equiv 1 \pmod{3} \), and again a Euclid-style proof finishes the argument.

9. (a) The congruence \( y^2 \equiv x^2 + k \pmod{p} \) is equivalent to \( (y-x)(y+x) \equiv k \pmod{p} \). Let \( z = y - x, w = y + x \). Note that since \( p \) is odd, we can invert this system to solve for \( x, y \):

\[
\begin{cases} x \equiv \frac{w-z}{2} \pmod{p} \\ y \equiv \frac{w+z}{2} \pmod{p} \end{cases}
\]

So the number of solutions to \( y^2 \equiv x^2 + k \pmod{p} \) is the same as the number of solutions to \( zw \equiv k \pmod{p} \). Now we can choose any nonzero value for \( z \) and let \( w = k/z \). Therefore there are exactly \( p-1 \) solutions.

(b) The number of solutions to \( y^2 \equiv x^2 + k \pmod{p} \), for a fixed value of \( x \), is \( 1 + \left( \frac{x^2+k}{p} \right) \). So

\[
p - 1 = \sum_{x=1}^{p} \left[ 1 + \left( \frac{x^2+k}{p} \right) \right] = p + \sum_{x=1}^{p} \left( \frac{x^2+k}{p} \right).
\]

Thus,

\[
\sum \left( \frac{x^2+k}{p} \right) = -1.
\]
(c) The number of solutions to $ax^2 + by^2 \equiv 1 \pmod{p}$ is

$$
\sum_{x=1}^{p} \left[ 1 + \left( \frac{1 - ax^2}{p} \right) \right] = p + \sum \left( \frac{1 - ax^2}{p} \right) \frac{b^{-1}}{p} \\
= p + \sum \left( \frac{1 - ax^2}{p} \right) \frac{b}{p} \\
= p + \sum \left( \frac{x^2 - 1/a}{p} \right) \frac{(-a)}{p} \frac{b}{p} \\
= p + \left( \frac{-ab}{p} \right) \sum \left( \frac{x^2 - a^{-1}}{p} \right) \\
= p - \left( \frac{-ab}{p} \right),
$$

where the last equality follows from part (a).

10. You should observe that for primes congruent to 1 mod 4, $R = N$, whereas for primes congruent to 3 mod 4, $R > N$. When $p \equiv 1 \pmod{4}$, $R = N$ follows easily from observing that if $x$ is a quadratic residue then so is $p - x$, so the number of quadratic residues in $\{1, \ldots, \frac{p-1}{2}\}$ must be $\frac{p-1}{4}$, exactly half of the total number of quadratic residues. When $p \equiv 3 \pmod{4}$, no elementary proof that $R > N$ is known. (The known proof uses L-functions and Dirichlet’s class number formula.)

11. First, it’s easy to see that all the quadratic residues must lie in $S_1$, because for all $x \in \{1, \ldots, p - 1\}$, $x$ lies in the same set as itself, so $x^2$ lies in $S_1$. Since $S_2$ is nonempty it must contain some quadratic nonresidue $u \pmod{p}$. Moreover, the $\frac{p-1}{2}$ elements in the set $\{ur : r \text{ a quadratic residue}\}$ must all lie in $S_2$ because $u \in S_2$ and $r \in S_1$. We’ve now exhausted all the nonzero residue classes of $p$, so $S_1$ contains all the residues and $S_2$ all the nonresidues.

12. (a) Note that $\pi s_i(i) = \pi (s_i(i)) = \pi(i + 1)$, $\pi s_i(i + 1) = \pi (s_i(i + 1)) = \pi(i)$, and for $j \neq i, i + 1$ we have $\pi s_i(j) = \pi (s_i(j)) = \pi(j)$. Now if $j, k \not\in \{i, i + 1\}$ then $\pi(j) = \pi s_i(j)$ and $\pi(k) = \pi s_i(k)$ so $(j, k)$ is an inversion of $\pi$ if and only if it is an inversion of $\pi s_i$. So the changes in inversions happen in one of the following three cases:

Case I: $(i, i + 1)$

Case II: $(j, i)$ or $(j, i + 1)$, where $j < i$

Case III: $(i, k)$ or $(i + 1, k)$, where $k > i + 1$.

Now for case II, we see that $(j, i)$ is an inversion of $\pi$ if and only if $(j, i + 1)$ is an inversion of $\pi s_i$, and $(j, i + 1)$ is an inversion of $\pi$ if and only if $(j, i)$ is an inversion of $\pi s_i$. So the total number of inversions in case II doesn’t change between $\pi$ and $\pi s_i$. Similarly, the total number of inversions doesn’t change in Case III. Case I only involves one pair $(i, i + 1)$, and thus the number of inversions changes by exactly $\pm 1$.

(b) We use proof by induction on the number of inversions in the permutation $\pi$. If $\pi$ has no inversions then $\pi$ must be the identity, and is thus an empty product of transpositions. So assume $\pi$ has $k$ inversions, and we’ve proved the result for all permutations with fewer than $k$ inversions. Let $(i, i + 1)$ be an inversion of $\pi$. Then $\pi s_i$ has one fewer inversion, so by the inductive hypothesis, $\pi s_i = s_{j_1} s_{j_2} \cdots s_{j_t}$ is a product of transpositions. Since $s_i^2 = 1$, we have that $\pi = \pi s_i^2 = s_{j_1} \cdots s_{j_t} s_i$ is also a product of transpositions, completing the induction.

(c) It’s enough to show that $\text{sign}(\pi s_i) = \text{sign}(\pi) \text{sign}(s_i)$ for any transposition $s_i$ and permutation $\pi$. Once we do this, it follows by induction that

$$
\text{sign}(s_{i_1} \cdots s_{i_r}) = \text{sign}(s_{i_1}) \cdots \text{sign}(s_{i_r}) = (-1)^r,
$$

so if $\pi = s_{i_1} \cdots s_{i_r}$ and $\sigma = s_{j_1} \cdots s_{j_t}$, then $\pi \circ \sigma = s_{i_1} \cdots s_{i_r} s_{j_1} \cdots s_{j_t}$ and hence $\text{sign}(\pi \circ \sigma) = (-1)^{r+t} = \text{sign}(\pi) \text{sign}(\sigma)$. 

4
Now by part (a), the number of inversions of $\pi s_i$ is the number of inversions of $\pi$ plus or minus 1. So if we define $f(\rho)$ to be the number of inversions of a permutation $\rho$, then

$$\text{sign}(\pi s_i) = (-1)^{f(\pi s_i)}$$
$$= (-1)^{f(\pi)}(-1)^{\pm 1}$$
$$= \text{sign}(\pi)\text{sign}(s_i).$$

(d) The proof is by induction on $k$. For the base case $k = 2$, we have the transposition $\pi = (ab)$ where we can assume without loss of generality that $a < b$. Now the number of inversions is $2(b - a - 1) + 1$, which is odd, so $\text{sign}(\pi) = -1 = (-1)^{2-1}$.

Next, consider an arbitrary $k$-cycle $\pi = (a_1 \cdots a_k)$. Since $\pi = (a_1 \cdots a_{k-1})(a_{k-1}a_k)$, by the inductive hypothesis

$$\text{sign}(\pi) = (-1)^{k-2}(-1) = (-1)^{k-1}.$$ 

This completes the induction. Therefore, for a disjoint product of cycles, the sign is $(-1)^m$, where $m$ is the number of even-length cycles.