Math 255 - Spring 2017
Homework 11 Solutions

1. To solve an equation of the form $x^2 \equiv a \pmod{n}$, we must factor n into its prime power factors $n = p_1^{k_1} \dots p_r^{k_r}$, solve $x^2 \equiv a \pmod{p_i^{k_i}}$ for each prime power factor and then "glue" every possible choice of one solution modulo each $p_i^{k_i}$ using the Chinese Remainder Theorem to obtain the solutions modulo n.

   In concrete terms, since $63 = 3^2 \cdot 7$, here we solve $x^2 \equiv 7 \pmod{9}$ and $x^2 \equiv 7 \pmod{7}$ then build the solutions modulo 63 using the Chinese Remainder Theorem from each choice of one solution modulo 9 and one solution modulo 7.

   $\underline{x^2 \equiv 7 \pmod{9}}$: To solve $x^2 \equiv 7 \pmod{9}$ we lift a solution to $x^2 \equiv 7 \pmod{3}$. Since $7 \equiv 1 \pmod{3}$, this is the equation $x^2 \equiv 1 \pmod{3}$, which has the solution $x_0 \equiv 1 \pmod{3}$.

   We are therefore looking for x_1 such that
$$x_1 = 1 + 3y_0$$
   (this ensures that x_1 is a lift of 1 modulo 3) and
$$x_1^2 \equiv 7 \pmod{9}$$
   (this ensures that we are solving our equation).

   We have
$$\begin{aligned} x_1^2 &= (1+3y_0)^2 \\ &= 1 + 6y_0 + 9y_0^2 \\ &\equiv 1 + 6y_0 \pmod{9}. \end{aligned}$$

   Therefore we want to solve
$$\begin{aligned} x_1^2 \equiv 1 + 6y_0 &\equiv 7 \pmod{9} \\ 6y_0 &\equiv 6 \pmod{9}. \end{aligned}$$

   Since 6 is not a unit modulo 9, we divide through by $\gcd(6, 9) = 3$ to get the equation
$$2y_0 \equiv 2 \pmod{3}$$
   which has solution $y_0 \equiv 1 \pmod{3}$. Therefore the solution is $x_1 = 1 + 3 = 4$.

   The two solutions to the equation are $x \equiv 4 \pmod{9}$ and $x \equiv -4 \equiv 5 \pmod{9}$.

   $\underline{x^2 \equiv 7 \pmod{7}}$: We now solve $x^2 \equiv 7 \pmod{7}$. This is the equation $x^2 \equiv 0 \pmod{7}$, which has the unique solution $x \equiv 0 \pmod{7}$, since the ring $\mathbb{Z}/7\mathbb{Z}$ does not have zero divisors.

Chinese Remainder Theorem step: To solve the equation modulo 63, we now use the Chinese Remainder Theorem to build the congruences class modulo 63 that satisfies

$$x \equiv 4 \pmod{9} \quad \text{and} \quad x \equiv 0 \pmod{7}$$

and the congruence class modulo 63 that satisfies

$$x \equiv 5 \pmod{9} \quad \text{and} \quad x \equiv 0 \pmod{7}.$$

(This is every possible choice of one solution modulo 9 and one solution modulo 7.)

We first tackle the first problem. In the notation of the Chinese Remainder Theorem we have $a_1 = 4$, $N_1 = 7$ and to find x_1 we must solve $N_1 x_1 \equiv 1 \pmod{9}$ or $7x_1 \equiv 1 \pmod{9}$. Using Euclid's algorithm we have

$$\begin{aligned} 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1. \end{aligned}$$

And so

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3(9 - 7) \\ &= 7 - 3 \cdot 9 + 3 \cdot 7 \\ &= 4 \cdot 7 - 3 \cdot 9. \end{aligned}$$

Therefore $7^{-1} \equiv 4 \pmod{9}$ and we can use $x_1 = 4$.

Continuing with our first Chinese Remainder Theorem problem, we also have $a_2 = 0$, so it doesn't matter what N_2 and x_2. Our unique solution is thus

$$x \equiv 4 \cdot 7 \cdot 4 + 0 \equiv 112 \equiv 49 \pmod{63},$$

and this is our first solution to the quadratic equation $x^2 \equiv 7 \pmod{63}$.

We now do the second Chinese Remainder Theorem: This time we have $a_1 = 5$, $N_1 = 7$ and $N_1 x_1 \equiv 1 \pmod{9}$. Since this is the same equation as above, we can reuse $x_1 = 4$. We still have $a_2 = 0$. In other words, only a_1 is different from the first CRT problem so it's not too bad. Our second solution is thus

$$x \equiv 5 \cdot 7 \cdot 4 + 0 \equiv 140 \equiv 14 \pmod{63}.$$

The two solutions to $x^2 \equiv 7 \pmod{63}$ are $x \equiv 14 \pmod{63}$ and $x \equiv 49 \pmod{63}$.

2. In this problem we will be solving the general quadratic equation $ax^2 + bx + c \equiv 0 \pmod{n}$. To do this, we use the quadratic formula

$$x \equiv \frac{-b + \text{``}\sqrt{b^2 - 4ac}\text{''}}{2a} \pmod{n},$$

where division by $2a$ is multiplication by $(2a)^{-1}$ and "$\sqrt{b^2 - 4ac}$" denotes a choice of a solution to the equation $y^2 \equiv b^2 - 4ac \pmod{n}$. There are as many solutions x to the general quadratic equation as there are solutions y to the simple quadratic congruence $y^2 \equiv b^2 - 4ac \pmod{n}$.

(a) For this equation $a = 1$, $b = 5$, and $c = 6$. Therefore the quadratic formula is

$$x \equiv \frac{-5 + \text{``}\sqrt{25 - 4 \cdot 1 \cdot 6}\text{''}}{2} \equiv \frac{-5 + \text{``}\sqrt{1}\text{''}}{2} \pmod{125}.$$

Therefore our first order of business is to solve $y^2 \equiv 1 \pmod{125}$. In general, we would use the technique used in problem 1, but this problem is simpler. First, n is already a power of an odd prime, so there is no need for the Chinese Remainder Theorem. Second, although we could solve the equation modulo 5 and lift, in this case 1 is a square in the integers and we already know two solutions to this equation: $y \equiv 1 \pmod{125}$ and $y \equiv -1 \pmod{125}$. Since n is a power of an odd prime, we know $y^2 \equiv 1 \pmod{125}$ has two solutions by Theorem 9.11, so these must be it.

Therefore, going back to the quadratic formula, the two solutions are

$$x \equiv \frac{-5 + 1}{2} \equiv \frac{-4}{2} \equiv -2 \equiv 123 \pmod{125}$$

and

$$x \equiv \frac{-5 - 1}{2} \equiv \frac{-6}{2} \equiv -3 \equiv 122 \pmod{125}.$$

In both cases we can divide by 2 since 2 is a unit modulo 125.

(b) This time $a = 1$, $b = 1$, and $c = 3$. Therefore the quadratic formula is

$$x \equiv \frac{-1 + \text{``}\sqrt{1 - 4 \cdot 1 \cdot 3}\text{''}}{2} \equiv \frac{-5 + \text{``}\sqrt{-11}\text{''}}{2} \pmod{27}.$$

We start by solving $y^2 \equiv -11 \pmod{27}$. Again, in general, we would use the technique used in problem 1, but this problem turns out to be simple as in part (a) above. First, n is already a power of an odd prime, so there is no need for the Chinese Remainder Theorem. Second, although we could solve the equation modulo 3 and lift, if we notice that $-11 \equiv 16 \pmod{27}$, then we are in the same situation as in part a), and by the same reasoning as in part a), the two solutions are $y \equiv 4 \pmod{27}$ and $y \equiv -4 \pmod{27}$. These are the only solutions since 27 is a power of an odd prime.

Therefore, going back to the quadratic formula, the two solutions are

$$x \equiv \frac{-1+4}{2} \equiv \frac{3}{2} \pmod{27}$$

and

$$x \equiv \frac{-1-4}{2} \equiv \frac{-5}{2} \pmod{27}.$$

This time to divide by 2 we must compute 2^{-1} modulo 27. Since $2 \cdot 14 = 28 \equiv 1 \pmod{27}$, $2^{-1} \equiv 14 \pmod{27}$. Therefore the solutions are

$$x \equiv \frac{-3}{2} \equiv 14 \cdot 3 \equiv 42 \equiv 15 \pmod{27}$$

and

$$x \equiv \frac{-5}{2} \equiv 14 \cdot (-5) \equiv -70 \equiv 11 \pmod{27}.$$

3. (a) Let $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ be the factorization of n into primes, where $k_0 \geq 0$ and each $k_i \geq 1$ for $i = 1, \dots, r$. As in problem 1, we must first solve $x^2 \equiv 1 \pmod{p_i^{k_i}}$ for each prime power $p_i^{k_i}$ dividing n, and then figure out how many ways these can be put together into a solution modulo n.

The case of n odd ($k_0 = 0$): We note that for each odd p_i, the equation

$$x^2 \equiv 1 \pmod{p_i^{k_i}}$$

has exactly two solutions by Theorem 9.11 because $\left(\frac{1}{p_i}\right) = 1$.

When we do the Chinese Remainder Theorem step, for each prime dividing n, we have to choose one of two solutions modulo $p_i^{k_i}$ to get one solution modulo each $p_i^{k_i}$ to "glue" together to make one solution modulo n. Therefore, if n is odd, there are $2^r = 2^{\omega(n)}$ solutions to $x^2 \equiv 1 \pmod{n}$, because in this case $r = \omega(n)$.

The case of $\gcd(n, 8) = 2$ ($k_0 = 1$): If $k_0 = 1$, then there is one solution to $x^2 \equiv 1 \pmod{2}$ by Theorem 9.12. This time, when we do the Chinese Remainder Theorem step, modulo 2 we only have one choice and for each **odd** prime dividing n, we have two choices for a solution modulo $p_i^{k_i}$; this gives us 2^r different ways to choose to get one solution modulo each prime power factor of n that can be "glued" together to make one solution modulo n. Therefore, there are again 2^r solutions to the equation $x^2 \equiv 1 \pmod{n}$, but this time $\omega(n) = r + 1$ since 2 is another prime dividing n (in addition to the r odd primes). Therefore $x^2 \equiv 1 \pmod{n}$ has $2^{\omega(n)-1}$ solutions.

The case of $\gcd(n, 8) = 4$ ($k_0 = 2$): If $k_0 = 2$, then there are two solutions to $x^2 \equiv 1 \pmod{4}$ by Theorem 9.12, and still two solutions to $x^2 \equiv 1 \pmod{p_i^{k_i}}$ when p_i is odd. Therefore there are $2 \cdot 2^r = 2^{r+1}$ solutions to the equation $x^2 \equiv 1 \pmod{n}$, and since $\omega(n) = r + 1$, $x^2 \equiv 1 \pmod{n}$ has $2^{\omega(n)}$ solutions.

The case of $\gcd(n, 8) = 8$ ($k_0 \geq 3$): Finally, if $k_0 \geq 3$, there are four solutions to $x^2 \equiv 1 \pmod{2^{k_0}}$ by Theorem 9.12. Therefore there are $4 \cdot 2^r = 2^{r+2} = 2^{\omega(n)+1}$ solutions to the equation $x^2 \equiv 1 \pmod{n}$.

Therefore we have

$$f(n) = \begin{cases} 2^{\omega(n)-1} & \text{if } \gcd(n, 8) = 2, \\ 2^{\omega(n)} & \text{if } \gcd(n, 8) = 1 \text{ or } \gcd(n, 8) = 4, \\ 2^{\omega(n)+1} & \text{if } \gcd(n, 8) = 8. \end{cases}$$

(b) For any $n > 1$, $\omega(n) \geq 1$ (every number is divisible by at least one prime), so both $2^{\omega(n)}$ and $2^{\omega(n)+1}$ are always even. However, $f(n) = 2^{\omega(n)-1} = 1$ when n is divisible by exactly one prime and $\gcd(n, 8) = 2$. If $\gcd(n, 8) = 2$, then n is divisible by 2. Since 2 is a prime, this is the only prime dividing n. However, if $\gcd(n, 8) = 2$ and $n = 2^{k_0}$, it must be that $k_0 = 1$, or $n = 2$. Therefore, $f(2) = 1$, and otherwise $f(n)$ is even.

(c) We note that when $n = 2$, $\prod_{a \in (\mathbb{Z}/2\mathbb{Z})^\times} a \equiv 1 \equiv -1 \pmod 2$ (although the question asked to assume that $f(n)$ is even, so we do not need to consider $n = 2$).

Now we must determine when $f(n)/2$ is odd when $f(n)$ is even (i.e. $n \neq 2$). We consider each case in the formula for $f(n)$ separately.

If $\gcd(n, 8) = 8$, then $f(n)/2 = 2^{\omega(n)}$ and since $\omega(n) \geq 1$, $f(n)/2$ is always even in this case.

If $\gcd(n, 8) = 1$ or 4, then $f(n)/2 = 2^{\omega(n)-1}$, so $f(n)/2$ is odd if and only if $\omega(n) = 1$. If $\gcd(n, 8) = 4$, then $n = 4p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$. In this case if $\omega(n) = 1$, this forces $n = 4$. If $\gcd(n, 8) = 1$, then $n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ and each p_i is odd. In this case if $\omega(n) = 1$, this forces n to be a power of an odd prime.

Finally, if $\gcd(n, 8) = 2$, we exclude the case $n = 2$ because in this case $f(n)/2$ is not even. Therefore $n = 2p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ and $r \neq 0$ (i.e., n is divisible by at least one odd prime). Then $f(n)/2 = 2^{\omega(n)-2}$ is odd if and only if $\omega(n) = 2$. This forces $n = 2p^k$ for p an odd prime.

Therefore, we get that $f(n)/2$ is odd when $n = 4$, or $n = p^k$ or $n = 2p^k$ and p is an odd prime. As noted above, we can throw in $n = 2$ as well, and we get that $\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} a \equiv -1 \pmod n$ exactly when n has a primitive root. Fun!