Math 255 – Spring 2018
Solving $x^2 \equiv a \pmod m$

Contents

1 Lifting

We begin by recalling the definition of a lift of $a \pmod d$, since we will need it throughout.

Definition 1.1. Let n and d be two integers such that d divides n. Then b modulo n is a lift of a modulo d if

$$a \equiv b \pmod d.$$

A fixed congruence class a modulo d has $\frac{n}{d}$ different lifts modulo n, and they are given by

$$x \equiv a + dr \pmod n, \quad r = 0, 1, 2, \ldots, \frac{n}{d} - 1$$

Example 1.2. Let $n = 54$ and $d = 6$. Then $x \equiv 2 \pmod 6$ (so here $a = 2$) has $\frac{54}{6} = 9$ lifts modulo 54, and they are

$$x \equiv 2, 8, 14, 20, 26, 32, 38, 44, 50 \pmod{54}.$$

Note that all of these integers are different modulo 54, but they are all the same modulo 6.

2 Solving $x^2 \equiv a \pmod{p^k}$ for p odd

We begin with a proposition. This is the only time we will consider the case of $(a, p) > 1$:

Proposition 2.1. *The equation*

$$x^2 \equiv 0 \pmod p,$$

where p is any prime, has the unique solution $x \equiv 0 \pmod p$.

Proof. The only zero divisor in the ring $\mathbb{Z}/p\mathbb{Z}$ is 0. Therefore, if a product is 0, one of the factors must be 0, from which it follows that $x \equiv 0 \pmod p$. $\square$

Our main result is the following:

Theorem 2.2. *Let p be an odd prime and $a \in \mathbb{Z}$ with $(a, p) = 1$. The equation*

$$x^2 \equiv a \pmod{p^k}$$

either

- *has no solution if $\left(\frac{a}{p}\right) = -1$; or*
- *has 2 solutions x_1 and $-x_1$ if $\left(\frac{a}{p}\right) = 1$.*

Proof. If $x^2 \equiv a \pmod{p^k}$ has a solution, say we call it b, then b is also a solution to $x^2 \equiv a \pmod{p}$, by simply "reducing more." (Alternatively we can argue that if p^k divides $b^2 - a$, then p divides $b^2 - a$ as well.) Therefore if $x^2 \equiv a \pmod{p^k}$ has a solution, then so does $x^2 \equiv a \pmod{p}$. The contrapositive of this statement is that if $x^2 \equiv a \pmod{p}$ does not have a solution, then $x^2 \equiv a \pmod{p^k}$ does not have a solution. This takes care of almost all of the theorem, except the claim that there are exactly two solutions if there is a solution.

Suppose now that $x^2 \equiv a \pmod{p^k}$ has a solution, say $x \equiv x_1 \pmod{p^k}$. We can easily show that $-x_1$ is also a solution of this equation, since $(-x_1)^2 \equiv x_1^2 \equiv a \pmod{p^k}$. Therefore it remains to show that this is the only other solution of this equation when there is a solution. We note, as we will need it later, that if $(a, p) = 1$, then also $(x_1, p) = 1$, because if that were not the case then certainly also (a, p) would be greater than 1, since $x_1^2 \equiv a \pmod{p}$.

Let b be any other solution of the equation $x^2 \equiv a \pmod{p^k}$. Then we have that

$$x_1^2 - b^2 \equiv (x_1 - b)(x_1 + b) \equiv 0 \pmod{p^k}.$$

Since p^k is not a prime, we cannot conclude yet that p^k divides $x_1 - b$ or p^k divides $x_1 + b$; we must show it. Assume instead that there is ℓ such that p^ℓ divides $x_1 - b$ and $p^{k-\ell}$ divides $x_1 + b$, so that p^k divides $(x_1 - b)(x_1 + b)$. We'll write $x_1 - b = sp^\ell$ and $x_1 + b = tp^{k-\ell}$, for s and t integers. From this it follows, with some arithmetic manipulations, that

$$2b = tp^{k-\ell} - sp^\ell.$$

Suppose that $0 < \ell < k$, so that both ℓ and $k - \ell$ are positive. In that case, p divides the right hand side of the equation above. However, we have that $(2, p) = 1$, since p is odd and $(b, p) = 1$ since b is a solution of $x^2 \equiv a \pmod{p}$, with $(a, p) = 1$. Therefore $(2b, p) = 1$, and we have a contradiction.

It must thus be the case that either $\ell = 0$, in which case p^k divides $x_1 + b$, which we can write as $x_1 + b \equiv 0 \pmod{p^k}$, or $b \equiv -x_1 \pmod{p^k}$. Otherwise, $\ell = k$, in which case p^k divides $x_1 - b$, and it follows that $b \equiv x_1 \pmod{p^k}$. This proves that the only possibilities for b a solution of $x^2 \equiv a \pmod{p^k}$ are for $b \equiv \pm x_1 \pmod{p^k}$.

□

We now turn our attention to finding the two solutions when they exist. The idea behind solving the equation is similar to induction:

1. We first solve the equation $x^2 \equiv a \pmod{p}$ (the "base case")

2. Given a solution to $x^2 \equiv a \pmod{p^j}$, we compute a solution to $x^2 \equiv a \pmod{p^{j+1}}$ (the "induction step"). We repeat this step, lifting our solution from modulo p to modulo p^2 to modulo p^3, until we get to the p^k that is our target.

The "base case" in our class will always be easy, either because p is small or because the equation is $x^2 \equiv 1, 4, 9, 16 \ldots \pmod{p}$ (which have a solution in the integers which also works modulo any prime p). We focus here on the lifting (or "induction") step.

Assume that we have a solution x_0 such that $x_0^2 \equiv a \pmod{p^j}$. Then we look for a lift of $x_0 \pmod{p^j}$ to $x_1 \pmod{p^{j+1}}$ that satisfies $x_1^2 \equiv a \pmod{p^{j+1}}$. Concretely, this gives us the following two equations:

1. The "lifting equation"
$$x_1 = x_0 + p^j y_0,$$
which ensures that $x_1 \pmod{p^{j+1}}$ is a lift of $x_0 \pmod{p^j}$,

2. and the equation
$$x_1^2 \equiv a \pmod{p^{j+1}},$$
which is the equation we are trying to solve.

Plugging the first equation into the second we get

$$\begin{aligned} a &\equiv (x_0 + p^j y_0)^2 \pmod{p^{j+1}} \\ &\equiv x_0^2 + 2x_0 p^j y_0 + p^{2j} y_0^2 \pmod{p^{j+1}} \\ &\equiv x_0^2 + 2x_0 p^j y_0 \pmod{p^{j+1}}. \end{aligned}$$

Recall that our unknown here is y_0. This is a linear equation in y_0. Furthermore, this equation can be shown to always have a unique solution $y_0 \pmod{p}$: Indeed we have

$$2x_0 p^j y_0 \equiv a - x_0^2 \pmod{p^{j+1}}.$$

Since $x_0^2 \equiv a \pmod{p^j}$, $a - x_0^2$ is divisible by p^j (this is, after all, the definition of what it means to be congruent). We also have that $(2x_0 p^j, p^{j+1}) = p^j$, since $(2x_0, p) = 1$ (p is odd, and x_0 cannot be divisible by p and be a solution to $x^2 \equiv a \pmod{p^j}$ if $\gcd(a, p) = 1$). Therefore we can divide all the way through by p^j and find the unique solution to

$$2x_0 y_0 \equiv \frac{a - x_0^2}{p^j} \pmod{p}$$

by multiplying both sides of the equation by $(2x_0)^{-1} \pmod{p}$ (which exists since $(2x_0, p) = 1$, as argued above).

3 Solving $x^2 \equiv a \pmod{2^k}$

We note that Proposition 2.1 still applies. Since $\gcd(a, 2) = 1$ implies that a is odd, we now restrict to this case. Our main result when $p = 2$ is the following:

Theorem 3.1. *Let a be odd. Then we have the following:*

1. *The equation*
$$x^2 \equiv a \pmod{2}$$
has the unique solution $x \equiv 1 \pmod{2}$.

2. *The equation*
$$x^2 \equiv a \pmod{4}$$
either
   - *has no solution if $a \equiv 3 \pmod{4}$; or*
   - *has two solutions $x \equiv 1, 3 \pmod{4}$ if $a \equiv 1 \pmod{4}$.*

3. *When $k \geq 3$, the equation*
$$x^2 \equiv a \pmod{2^k}$$
either
   - *has no solution if $a \not\equiv 1 \pmod{8}$; or*
   - *has four solutions x_1, $-x_1$, $x_1 + 2^{k-1}$, $-(x_1 + 2^{k-1})$ if $a \equiv 1 \pmod{8}$.*

We omit the proof of this theorem for now; it is similar to the proof of Theorem 2.2, except for a small technicality which gives 4 solutions instead of 2.

Since the cases of $k = 1$ and $k = 2$ are completely covered by the Theorem, we focus on the case of $k \geq 3$ and turn our attention to giving the four solutions in that case. The idea is identical to the one we used for p odd, except that we must modify the lifting step slightly. The base case is also easier.

1. We first solve the equation $x^2 \equiv a \pmod{8}$. Note that if there is a solution, then $a \equiv 1 \pmod{8}$, and therefore the "base case" is always solving $x^2 \equiv 1 \pmod{8}$. This has solutions $x \equiv 1, 3, 5, 7 \pmod{8}$ and we can choose to lift any of those four solutions.

2. Given a solution $x^2 \equiv a \pmod{2^j}$, we compute a solution to $x^2 \equiv a \pmod{2^{j+1}}$ (the "induction step"). We repeat this step, lifting our solution from modulo 8 to modulo 16 to modulo 32, until we get to the 2^k that is our target.

We now explain the lifting step or "induction" step.

Assume that we have a solution x_0 such that $x_0^2 \equiv a \pmod{2^j}$. Then we look for a lift of $x_0 \pmod{2^{j-1}}$ to $x_1 \pmod{p^{j+1}}$ that satisfies $x_1^2 \equiv a \pmod{p^{j+1}}$. Notice the small "backwards dance" that we must do for $p = 2$: We have a solution modulo 2^j, but when lifting we treat it as if it is a solution modulo 2^{j-1} (we "demote" it to $\mathbb{Z}/2^{j-1}\mathbb{Z}$) before lifting straight to $\mathbb{Z}/2^{j+1}\mathbb{Z}$. The reason we do this is the following: When we solve the equations as above, if we had

$$x_1 = x_0 + 2^j y_0,$$

and

$$x_1^2 \equiv a \pmod{2^{j+1}},$$

which are analogous to the equation we have when p is odd, then when we square, here is what happens:

$$\begin{aligned} a &\equiv (x_0 + 2^j y_0)^2 \pmod{2^{j+1}} \\ &\equiv x_0^2 + 2x_0 2^j y_0 + 2^{2j} y_0^2 \pmod{2^{j+1}} \\ &\equiv x_0^2 + 2^{j+1} x_0 y_0 \pmod{2^{j+1}} \\ &\equiv x_0^2 \pmod{2^{j+1}}. \end{aligned}$$

The variable y_0 has completely disappeared from the equation so we cannot solve for it! (There is also a more serious problem which we discuss in the Remarks below.)

Instead, this is what we do: We begin with the following two equations:

1. The "lifting equation"
$$x_1 = x_0 + 2^{j-1} y_0,$$
which ensures that $x_1 \pmod{2^{j+1}}$ is a lift of $x_0 \pmod{2^{j-1}}$,

2. and the equation
$$x_1^2 \equiv a \pmod{2^{j+1}},$$
which is the equation we are trying to solve.

Now we proceed as before: We plug the first equation into the second to get

$$\begin{aligned} a &\equiv (x_0 + 2^{j-1} y_0)^2 \pmod{2^{j+1}} \\ &\equiv x_0^2 + 2x_0 2^{j-1} y_0 + 2^{2j-2} y_0^2 \pmod{2^{j+1}} \\ &\equiv x_0^2 + 2^j x_0 y_0 \pmod{2^{j+1}}, \end{aligned}$$

where now the last term disappears since $2^{2j-2} \equiv 0 \pmod{2^{j+1}}$ because $2j - 2 \geq j + 1$ if $j \geq 3$ (which we have assumed to begin with since $k \geq 3$).

Again our unknown here is y_0 and this is a linear equation in y_0. Furthermore, this equation can be shown to always have a unique solution $y_0 \pmod 2$: Indeed we have

$$2^j x_0 y_0 \equiv a - x_0^2 \pmod{2^{j+1}}.$$

Since $x_0^2 \equiv a \pmod{2^j}$, again $a - x_0^2$ is divisible by 2^j. We also have that $\gcd(2^j x_0, 2^{j+1}) = 2^j$, since $\gcd(x_0, 2) = 1$ (x_0 cannot be divisible by 2 and be a solution to $x^2 \equiv a \pmod{2^j}$ if

$\gcd(a, 2) = 1$). Therefore we can divide all the way through by 2^j and find the unique solution to

$$x_0 y_0 \equiv y_0 \equiv \frac{a - x_0^2}{2^j} \pmod{2},$$

where here we use that $x_0 \equiv 1 \pmod{2}$ since $\gcd(x_0, 2) = 1$ so x_0 is odd.

Remark 3.2. We note that a quite important point has gotten swept under the rug: If

$$x_1 = x_0 + 2^{j-1} y_0,$$

then $0 \le y_0 < 4$ all give different lifts of $x_0 \pmod{2^{j-1}}$ to $x_1 \pmod{2^{j+1}}$. However, we have found $y_0 \pmod{2}$. Technically, we should find the two lifts of $y_0 \pmod{2}$ to $y_0 \pmod{4}$ to obtain **two** lifts of $x_0 \pmod{2^{j-1}}$ to $x_1 \pmod{2^{j+1}}$. However, for our procedure we only need one lift, and we find all solutions at the top level, once we have one solution to $x^2 \equiv a \pmod{2^k}$.

However, this is the reason why there are four solutions and why x_1 and $x_1 + 2^{k-1}$ are both solutions. These are both lifts of $x_1 \pmod{2^{k-2}}$ to $x_1 \pmod{2^k}$ that satisfy $x^2 \equiv a \pmod{2^k}$. We explain this with an example:

Example 3.3. Let us solve $x^2 \equiv 9 \pmod{32}$. We begin by solving $x^2 \equiv 9 \pmod{16}$, which has solutions $x \equiv 3, 5, 11, 13 \pmod{16}$ (we can find these by solving $x^2 \equiv 9 \pmod{8}$ and lifting, or by noticing that $x_1 = 3$ is a solution and using Theorem 3.1) . We now lift all of the solutions to see what we obtain:

First we lift $x_0 = 3$: We "demote" it to $x_0 = 3 + 8y_0$, then square:

$$\begin{aligned} 9 &\equiv (3 + 8y_0)^2 \pmod{32} \\ &\equiv 9 + 48y_0 + 64y_0^2 \pmod{32} \\ &\equiv 9 + 16y_0 \pmod{32}. \end{aligned}$$

We note that the equation

$$9 \equiv 9 + 16y_0 \pmod{32}$$

has the unique solution $y_0 \equiv 0 \pmod{2}$, but two solutions $y_0 \equiv 0, 2 \pmod{4}$ (and 16 solutions in $\mathbb{Z}/32\mathbb{Z}$ where this equation really lives!). This gives two different lifts of x_0:

$$x_1 \equiv 3 \pmod{32} \quad \text{and} \quad x_1 \equiv 19 \pmod{32}$$

of $x_0 \equiv 3 \pmod{8}$. We see that they are exactly of the form x_1 and $x_1 + 16$, as predicted by the theorem.

Now let us see what happens when we lift $x_0 = 5$. We "demote" to $x_0 = 5 + 8y_0$ then square:

$$\begin{aligned} 9 &\equiv (5 + 8y_0)^2 \pmod{32} \\ &\equiv 25 + 80y_0 + 64y_0^2 \pmod{32} \\ &\equiv 25 + 16y_0 \pmod{32}. \end{aligned}$$

We note that the equation

$$9 \equiv 25 + 16y_0 \pmod{32}$$

has the unique solution $y_0 \equiv 1 \pmod 2$, but two solutions $y_0 \equiv 1, 3 \pmod 4$. This gives two different lifts of x_0:

$$x_1 \equiv 13 \pmod{32} \quad \text{and} \quad x_1 \equiv 29 \pmod{32}$$

of $x_0 \equiv 5 \pmod 8$. Again these are of the form x_1 and $x_1 + 16$.

Finally, let us lift $x_0 = 11$: We "demote" it to $x_0 = 11 + 8y_0$, then square:

$$\begin{aligned} 9 &\equiv (11 + 8y_0)^2 \pmod{32} \\ &\equiv 121 + 176y_0 + 64y_0^2 \pmod{32} \\ &\equiv 25 + 16y_0 \pmod{32}. \end{aligned}$$

This is the same equation we obtained when we were lifting $x_0 = 5$, and it has solutions $y_0 \equiv 1, 3 \pmod 4$. This gives us the two lifts of x_0:

$$x_1 \equiv 19 \pmod{32} \quad \text{and} \quad x_1 \equiv 3 \pmod{32}.$$

We see that we obtained the same solutions as when we lifted $x_0 = 3$, which makes sense since $3 \equiv 11 \pmod 8$, so we were actually doing the same lift.

Similarly, if we were to lift $x_0 = 13$, we would get the solutions $x_1 \equiv 13 \pmod{32}$ and $x_1 \equiv 29 \pmod{32}$ again since $13 \equiv 5 \pmod 8$. This shows how each of four solutions can give two lifts that are solutions, but we still have only four solutions in total: There are two pairs of solutions that each give the same two lifts. If we chose $x_0 \pmod{16}$ and $-x_0 \pmod{16}$ two solutions of $x^2 \equiv 9 \pmod{16}$ and computed their four lifts (two lifts each) we would get all four solutions to $x^2 \equiv 9 \pmod{32}$.

Remark 3.4. We say here one more thing about the "demotion" of the solution modulo 2^j to a solution modulo 2^{j-1}. Looking at Example 3.3, we see that starting with the solution $x_0 \equiv 3 \pmod{16}$, we obtained the two solutions $x_1 \equiv 3 \pmod{32}$ and $x_1 \equiv 19 \pmod{32}$. These are both lifts of $3 \pmod{16}$. However, starting with the solution $x \equiv 5 \pmod{16}$, we obtained the two solutions $x_1 \equiv 13 \pmod{32}$ and $x_1 \equiv 29 \pmod{32}$. These are **not** lifts of $5 \pmod{16}$ (but they are lifts of $5 \pmod 8$, of course). In fact, all of the solutions of $x^2 \equiv 9 \pmod{32}$ are lifts of $3 \pmod{16}$ and $13 \pmod{16}$, and none are lifts of $5 \pmod{16}$ or $11 \pmod{16}$. However, we have that $3 \equiv 11 \pmod 8$ and $13 \equiv 5 \pmod 8$, so by demoting down to $\pmod 8$, we ensure that we can now lift all of the solutions. This is good because before we solve the equation we cannot know which solutions $\pmod{16}$ lift to $\pmod{32}$.

This is why, incidentally, we cannot lift directly from a solution to $x^2 \equiv 9 \pmod 8$ to a solution to $x^2 \equiv 9 \pmod{32}$. If I choose x_0 a solution of $x^2 \equiv 9 \pmod 8$, say for example $x_0 \equiv 1 \pmod 8$, if I am unlucky x_0 might not be a solution of $x^2 \equiv 9 \pmod{16}$ and therefore it will certainly not lift to a solution of $x^2 \equiv 9 \pmod{32}$. To avoid this situation, I start by choosing a solution x_0 to $x^2 \equiv 9 \pmod{16}$, then I demote it down to a solution of $x^2 \equiv 9$

(mod 8) but now since I know that I can lift to a solution to $x^2 \equiv 9 \pmod{16}$, I know that I will not be unlucky and I can also lift to a solution to $x^2 \equiv 9 \pmod{32}$.

To be explicit:

$$x^2 \equiv 9 \pmod{8}$$

has the four solutions $x \equiv 1, 3, 5, 7 \pmod{8}$. Of these, only two lift to solutions to

$$x^2 \equiv 9 \pmod{16},$$

namely $x \equiv 3 \pmod{8}$ and $x \equiv 5 \pmod{8}$ lift to $x \equiv 3, 11 \pmod{16}$ and $x \equiv 5, 13 \pmod{16}$ respectively.

Then the same thing happens at the next step: Of the four solutions $x \equiv 3, 5, 11, 13 \pmod{16}$ of the equation

$$x^2 \equiv 9 \pmod{16},$$

only $x \equiv 3 \pmod{16}$ and $x \equiv 13 \pmod{16}$ actually lift to solutions to

$$x^2 \equiv 9 \pmod{32},$$

which has solutions $x \equiv 3, 13, 19, 23 \pmod{32}$.

The reason things are so messed up, and different from the case of p odd, where every solution modulo p^j lifts to a solution modulo p^{j+1}, is because the derivative of x^2 is $2x$ which is identically zero modulo 2. The deeper reason why this matters involves studying p-adic integers and Hensel's Lemma, which tells you exactly when solutions modulo p^j to any equation lift uniquely to a solution modulo p^{j+1}.

4 Solving $x^2 \equiv a \pmod{m}$ for general m

To do this we use the Chinese Remainder Theorem. Let $m = p_1^{e_1} \dots p_k^{e_k}$. Suppose that we have a number x such that

$$x^2 \equiv a \pmod{p_i^{e_i}}$$

for each prime power factor $p_i^{e_i}$ of m. Then by changing variables to $y = x^2$, we have that

$$y \equiv a \pmod{p_i^{e_i}}$$

and therefore by the Chinese Remainder Theorem

$$y \equiv a \pmod{m}$$

or $x^2 \equiv a \pmod{m}$.

Now at the same time, suppose that we have a k-tuple $(a_1, a_2, \dots, a_k)$ such that for each i

$$a_i^2 \equiv a \pmod{p_i^{e_i}},$$

then there is a unique congruence class $x \pmod{m}$ such that

$$x \equiv a_i \pmod{p_i^{e_i}}.$$

This explains why we may solve the equation $x^2 \equiv a \pmod{m}$ "prime power by prime power."

Example 4.1. Let us solve the equation

$$x^2 \equiv 1 \pmod{72}.$$

Since $72 = 2^3 \cdot 3^3$, we must solve

$$x^2 \equiv 1 \pmod{8} \quad \text{and} \quad x^2 \equiv 1 \pmod{9}.$$

In general, we would need to use the techniques of Sections 2 and 3, since these are equations of the form $x^2 \equiv a \pmod{p^k}$. However, these equations are particular simple so we are not required to do applying the lifting technique.

The equation $x^2 \equiv 1 \pmod{8}$ has solutions $x \equiv 1, 3, 5, 7 \pmod{8}$, as we know.

The equation $x^2 \equiv 1 \pmod{9}$ has one solution $x_1 \equiv 1 \pmod{9}$. By Theorem 2.2, this equation has two solutions and the other solution is $-x_1 \equiv -1 \equiv 8 \pmod{9}$.

Therefore, for any pair (a_1, a_2) such that $a_1^2 \equiv 1 \pmod{8}$ and $a_2^2 \equiv 1 \pmod{9}$, we get one solution to $x^2 \equiv 1 \pmod{72}$. There are 8 such pairs:

$$(1,1), \quad (1,8), \quad (3,1), \quad (3,8), \quad (5,1), \quad (5,8), \quad (7,1), \quad \text{and} \quad (7,8).$$

Each pair gives a solution in the following way. In the notation of the Chinese Remainder Theorem, we have $a_1 = 5$, $M_1 = 9$ and $x_1 = 1$ and $a_2 = 1$, $M_2 = 8$ and $x_2 = -1$.

Suppose we take the pair $(5, 1)$, this stands for the Chinese Remainder Theorem problem

$$x \equiv 5 \pmod{8}, \quad x \equiv 1 \pmod{9}.$$

Therefore we get the solution

$$x \equiv 5 \cdot 9 \cdot 1 + 1 \cdot 8 \cdot (-1) \equiv 37 \pmod{72}.$$

If we take the pair $(7, 1)$, this is the pair of equations

$$x \equiv 7 \pmod{8}, \quad x \equiv 1 \pmod{9}.$$

Therefore we get the solution

$$x \equiv 7 \cdot 9 \cdot 1 + 1 \cdot 8 \cdot (-1) \equiv 55 \pmod{72}.$$

In this manner we can get the 8 solutions $x \equiv 1, 17, 19, 35, 37, 53, 55, 71 \pmod{72}$ quite quickly.