Math 255 – Spring 2017
Solving $x^2 \equiv a \pmod{n}$

Contents

1 Lifting

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.

Note that the notion of lifting has come up earlier in the semester without us giving it this name:

1. When we solve a linear equation $ax \equiv b \pmod{n}$ but $\gcd(a, n) > 1$, if $\gcd(a, n)$ divides b we "divide everything" by $\gcd(a, n)$. This gives us an equation $a'x \equiv b' \pmod{n'}$, with
$$a' = \frac{a}{\gcd(a, n)}, \quad b' = \frac{b}{\gcd(a, n)}, \quad n = \frac{n}{\gcd(a, n)},$$
and now $\gcd(a', n') = 1$. Therefore $a'^{-1} \pmod{n'}$ exists and the equation can be solved by division to give a unique solution x' modulo n'. Then the solutions of the original equation, are exactly all of the lifts $x \pmod{n}$ of $x' \pmod{n'}$.

   Example 1.3. Let's solve
$$15x \equiv 39 \pmod{42}.$$
Since $\gcd(15, 42) = 3$, 15 is not a unit modulo 42. Furthermore, since 3 divides 39, the equation has $\gcd(15, 42) = 3$ solutions. (If 3 did not divide 39, we could not

"divide everything" by 3 and there would be no solution, see Theorem 4.7.) We start by dividing all the way through:

$$5x \equiv 13 \pmod{14}.$$

Now 5 is a unit modulo 14, with inverse 3, since $5 \cdot 3 = 15 \equiv 1 \pmod{14}$ (there is no relation between this 3 and the $\gcd(15, 42)$, this is a coincidence). We multiply both sides by 3

$$x \equiv 39 \equiv 11 \pmod{14}$$

to solve the equation. The three solutions modulo 42 are the three lifts of $x \equiv 11 \pmod{14}$ to $\mathbb{Z}/42\mathbb{Z}$:

$$x \equiv 11 + 14r, \quad r = 0, 1, 2$$

or

$$x \equiv 11, 25, 39 \pmod{42}.$$

2. The Chinese Remainder Theorem is an example of when we can be guaranteed to obtain a unique simultaneous lift of several congruences. Given

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k}$$

with the n_is pairwise relatively prime, we are told that there is a unique lift

$$x \equiv a \pmod{n},$$

where $n = n_1 n_2 \cdots n_k$, that lifts simultaneously all of the congruence classes listed.

Example 1.4. Consider the set of congruences

$$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7};$$

this problem Section 4.4, problem 4(a). These three congruences lift to a unique class modulo $n = 3 \cdot 5 \cdot 7 = 105$:

$$x \equiv 52 \pmod{105}.$$

We can check that this is a lift of each of the congruences: Indeed

$$\begin{gathered} 52 \equiv 1 \pmod{3}, \\ 52 \equiv 2 \pmod{5}, \quad \text{and} \\ 52 \equiv 3 \pmod{7}. \end{gathered}$$

The reason why the Chinese Remainder Theorem requires that the n_is be relatively prime is so that the congruences do not contradict each other. There is no problem if $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$ with $\gcd(n_1, n_2) > 1$, as long as both a_1 and a_2 are lifts of the same congruence class modulo $\gcd(n_1, n_2)$. In that case there is a unique lift to

$$x \equiv a \pmod{\operatorname{lcm}(n_1, n_2)}.$$

Otherwise there is no lift.

Example 1.5. Consider the two congruences

$$x \equiv 4 \pmod 6 \quad \text{and} \quad x \equiv 10 \pmod{15}.$$

Since $\gcd(6, 15) = 3$, this will have a common lift modulo $\operatorname{lcm}(6, 15) = 30$ if and only if

$$4 \equiv 10 \pmod 3.$$

Since this is the case the lift exists. We can compute it using the Chinese Remainder Theorem as the simultaneous lift of

$$x \equiv 0 \pmod 2, \quad \text{and} \quad x \equiv 10 \pmod{15}$$

or

$$x \equiv 4 \pmod 6, \quad \text{and} \quad x \equiv 0 \pmod 5.$$

In any case the simultaneous lift is

$$x \equiv 10 \pmod{30}.$$

However, the two congruences

$$x \equiv 3 \pmod 6 \quad \text{and} \quad x \equiv 10 \pmod{15}$$

do not have a common lift to any modulus, since this would require at the same time that $x \equiv 0 \pmod 3$ and $x \equiv 1 \pmod 3$, which is impossible.

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 $\gcd(a, p) > 1$:

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 $x \equiv 0 \pmod p$. □

Our main result is the following:

Theorem 2.2 (Theorem 9.11)**.** *Let p be an odd prime and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. 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* $\left(\frac{a}{p}\right) = 1$.

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 $\gcd(2x_0 p^j, p^{j+1}) = p^j$, since $\gcd(2x_0, p) = 1$ (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 $\gcd(2x_0, p) = 1$, 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 (Theorem 9.12)**.** *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 $a \equiv 1 \pmod{8}$.*

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 $0 \leq y_0 < 4$ 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 $\pmod{32}$.

We note that this is exactly the problem we ran into in class when we tried to 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 $x^2 \equiv 9 \pmod 8$ 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 $x^2 \equiv a \pmod n$ for general n

To do this we use the Chinese Remainder Theorem. Let $n = p_1^{k_1} \dots p_r^{k_r}$. Suppose that we have a number x such that

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

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

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

and therefore by the Chinese Remainder Theorem

$$y \equiv a \pmod n$$

or $x^2 \equiv a \pmod n$.

Now at the same time, suppose that we have an r-tuple $(a_1, a_2, \dots, a_r)$ such that for each i

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

then there is a unique congruence class $x \pmod n$ such that

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

This explains why we may solve the equation $x^2 \equiv a \pmod n$ "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 $a_1 = 5$, $N_1 = 9$ and $x_1 = 1$ and $a_2 = 1$, $N_2 = 8$ 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.