

**Math 104B, Number Theory, Winter 2003.**

**Lecture 9. Solution of  $x^2 \equiv a \pmod{m}$ .**

**Example.** Solve  $x^2 \equiv 2 \pmod{641}$ .

**Solution.** We first check that 2 is a quadratic residue.

$$\left(\frac{2}{641}\right) = (-1)^{640 \cdot 642/8} = 1.$$

Now write  $641 - 1 = 2^7 \cdot 5 = 128 \cdot 5$ . We calculate

$$x_0 = 2^{(5+1)/2} = 2^3 = 8.$$

This satisfies

$$x_0^2 = 2^5 \cdot 2 = 32 \cdot 2.$$

We want to solve

$$y^{-2} \equiv 32 \pmod{641}.$$

What we know is that  $b_0 = 32$  has order dividing  $2^6 = 64$ . We choose a quadratic non-residue. Let's try  $n = 3$ .

$$\left(\frac{3}{641}\right) = (-1)^{(640/2)(2/2)} \left(\frac{641}{3}\right) = \left(\frac{2}{3}\right) = -1$$

so  $n = 3$  is a quadratic non-residue. We compute  $z = 3^5 = 243$ . Then the elements whose orders divide 128 modulo 641 are given by the set

$$S_{128} = \{243, 243^2, 243^3, 243^4, \dots, 243^{128}\}.$$

If we can identify  $t$  such that  $32 \equiv 243^t$ , then  $t$  is even and  $243^{t/2}$  is a square root of 32, so  $y \equiv 243^{64-t/2} \pmod{641}$  satisfies

$$y^2 32 \equiv 243^{128-t} 32 \equiv 1 \pmod{641}.$$

It would be a lot of work to identify all the elements of  $S_{128}$  in order to locate 32. Instead we calculate the successive squares:

$k$	1	2	4	8	16	32	64	128
$243^k \pmod{641}$	243	77	160	601	318	487	640	1
order	128	64	32	16	8	4	2	1

The new idea we will use is the following Lemma

**Lemma 9.2.5.** Suppose  $b$  and  $c$  both have order  $2^m$  modulo  $p$  where  $p$  is prime. Then  $bc$  has order dividing  $2^{m-1}$ .

**Proof.**  $b^{2^{m-1}}$  and  $c^{2^{m-1}}$  both have order 2 modulo  $p$  and are therefore congruent to  $-1$ . Hence

$$(bc)^{2^{m-1}} \equiv (-1)(-1) \equiv 1 \pmod{p}.$$

We can think of  $c$  as being an approximate inverse for  $b$  modulo  $p$ . Now we apply this to find an approximate inverse for 32 whose square root we can compute. We need to find the precise order of 32 modulo 641.

$k$	1	2	4	8	16	32	64
$32^k \pmod{641}$	32	383	541	385	154	640	1

We see that the order is 64. An approximate inverse for 32 modulo 641 is thus 77, and the square root of 77 modulo 641 is 243. We set

$$x_1 \equiv 243 \cdot x_0 \equiv 243 \cdot 8 \equiv 21, \quad b_1 \equiv 77 \cdot b_0 \equiv 77 \cdot 32 \equiv 541.$$

Then

$$x_1^2 \equiv (243)^2 \cdot x_0^2 \equiv 77 \cdot b_0 \cdot 2 \equiv 541 \cdot 2 = b_1 \cdot 2.$$

What we have gained is that 541 now has smaller order than 32. In fact, we see that it has order 16. We can repeat this procedure again. An approximate inverse to 541 modulo 641 is 601 because this also has order 16. The square root of 601 modulo 641 is 160. We keep track of the calculations in the following table.

$i$	$x_i$	$b_i$	$\text{ord}_{641}(b_i)$
0	8	32	64
1	$243 \cdot 8 \equiv 21$	$77 \cdot 32 \equiv 541$	16
2	$160 \cdot 21 \equiv 155$	$601 \cdot 541 \equiv 154$	4
3	$318 \cdot 155 \equiv 67$	$487 \cdot 154 \equiv 1$	1

We see that the solution is  $x \equiv 67$ , and we check that indeed,  $67^2 = 7 \cdot 641 + 2$ .