

# Mathematics 115: The RESSOL Algorithm

Gagan Tara Nanda

24<sup>th</sup> October, 2003

## 1 Introduction

In this short article, we shall describe the algorithm RESSOL (which stands for RESidue SOLver) to find solutions to the congruence equation

$$x^2 \equiv a \pmod{p}. \quad (1)$$

The exposition follows the presentation in “An Introduction to the Theory of Numbers” by Niven, Zuckerman, and Montgomery. We hope the reader will be able to understand the material with minimal background knowledge of group theory and primitive roots.

## 2 Quadratic Congruences

We wish to solve congruences of the form  $x^2 \equiv a \pmod{p}$ . A question to ask is how many solutions (1) can have. We can show by induction that the congruence  $f(x) \equiv 0 \pmod{p}$  of degree  $q$  has at most  $q$  solutions. Let  $f(x) = x^2 - a$ , so that  $f(x)$  has degree  $q = 2$ . Then it is clear that (1) has at most 2 solutions. Can (1) have zero solutions? Consider the example  $x^2 \equiv 2 \pmod{5}$ . We can write any integer  $x$  in the form  $x \equiv 0, \pm 1, \pm 2 \pmod{5}$ . We have:

$$x \equiv 0 \pmod{5} \Rightarrow x^2 \equiv 0 \pmod{5}; \quad (2)$$

$$x \equiv \pm 1 \pmod{5} \Rightarrow x^2 \equiv 1 \pmod{5}; \quad (3)$$

$$x \equiv \pm 2 \pmod{5} \Rightarrow x^2 \equiv 4 \pmod{5}. \quad (4)$$

From (2) – (4) we see that the equation  $x^2 \equiv 2 \pmod{5}$  has no solutions. So indeed (1) need not have any solutions for a particular choice of  $a$  and  $p$ . What about 1 solution? Well, we note that if  $x$  is a solution to (1), then  $y = -x$  is also a solution, since

$$y^2 = (-x)^2 \equiv x^2 \pmod{p}.$$

This  $y$  is different from  $x$  because  $p$  is odd, so  $y \not\equiv x \pmod{p}$ . To see this, suppose  $y = -x \equiv x \pmod{p}$ . Then  $2x \equiv 0 \pmod{p}$ , which implies  $2x$  is an even multiple of  $p$ . But since  $0 < x < p$ , we have  $0 < 2x < 2p$ , and because there is no even multiple of  $p$  strictly between 0 and  $2p$ , we get a contradiction. Hence if (1) has a solution, it has two distinct solutions. So the congruence  $x^2 \equiv a \pmod{p}$  has either no solution, or exactly 2 solutions.

### 3 The RESSOL Algorithm

We want to find all solutions to the equation

$$x^2 \equiv a \pmod{p}. \quad (5)$$

We first find the highest power of 2 that divides  $p - 1$ ; that is, we wish to find  $k$  such that

$$p - 1 = 2^k \cdot m,$$

where  $m$  is clearly odd. Since the equation  $x^2 \equiv a \pmod{2}$  is easy to solve, we consider  $p > 2$ , which implies  $k > 0$ . We then set

$$r \equiv a^{\frac{m+1}{2}} \pmod{p}$$

and

$$n \equiv a^m \pmod{p}.$$

Now note that

$$\left(a^{\frac{m+1}{2}}\right)^2 = a^{m+1} = a \cdot a^m,$$

so

$$\begin{aligned} r^2 &\equiv \left(a^{\frac{m+1}{2}}\right)^2 \pmod{p} \\ &\equiv an \pmod{p}. \end{aligned} \quad (6)$$

Suppose first that  $n \equiv 1 \pmod{p}$ . Then (6) becomes

$$r^2 \equiv a \pmod{p},$$

so the two solutions to (5) are  $x \equiv \pm r \pmod{p}$ . Now suppose  $n \not\equiv 1 \pmod{p}$ . We first need a couple of definitions.

**Definition 1** Let  $(a, m) = 1$ . If the congruence  $x^2 \equiv a \pmod{m}$  has a solution, then  $a$  is called a quadratic residue modulo  $m$ .

**Definition 2** Let  $(a, m) = 1$ . If the congruence  $x^2 \equiv a \pmod{m}$  has no solution, then  $a$  is called a quadratic non-residue modulo  $m$ .

For instance, as we saw earlier,  $(2, 5) = 1$ , and the congruence  $x^2 \equiv 2 \pmod{5}$  has no solution. Thus 2 is a quadratic non-residue modulo 5. The following remark will also be useful, as will be the theorem that follows it. We state the theorem without proof verbatim from the text.

**Remark 3** Let  $(a, p) = 1$ , where  $p$  is a prime. Then  $a$  is a quadratic residue modulo  $p$  if and only if  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ .

**Theorem 4** If  $a$  and  $b$  are relatively prime to a prime number  $p$ , and if  $a$  and  $b$  both have order  $2^j \pmod{p}$  with  $j > 0$ , then  $ab$  has order  $2^{j'} \pmod{p}$  for some  $j' < j$ .

We now choose a quadratic non-residue  $z$  modulo  $p$ . This means that the congruence  $x^2 \equiv z \pmod{p}$  has no solution. Let  $c \equiv z^m \pmod{p}$ . Then we see that

$$c^{2^k} = (z^m)^{2^k} = z^{2^k m} = z^{p-1} \equiv 1 \pmod{p} \quad (7)$$

by Fermat's Little Theorem. Hence the order of  $c$  is a divisor of  $2^k$ . Moreover, we have

$$c^{2^{k-1}} = z^{2^{k-1} m} = z^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (8)$$

Note that the last step of (8) follows from **Remark 3**. Since the order of  $c$  is the smallest integer  $l$  such that for  $l' < l$  we have  $c^{l'} \not\equiv 1 \pmod{p}$  but  $c^l \equiv 1 \pmod{p}$ , we deduce that the order of  $c$  is in fact  $2^k$ . Similarly,

$$n^{2^k} = a^{2^k m} = a^{p-1} \equiv 1 \pmod{p},$$

so the order of  $n$  also divides  $2^k$ . Let this order be  $2^{k'}$ . Now observe that

$$n^{2^{k-1}} = a^{2^{k-1} m} = a^{\frac{p-1}{2}},$$

which implies that  $a$  is a quadratic residue modulo  $p$  if and only if  $n^{2^{k-1}} \equiv 1 \pmod{p}$ . This in turn is equivalent to the inequality  $k' < k$ . It is instructive to check that this is indeed true. Suppose not, so that  $k' = k$ . Then  $n^{2^k} \equiv 1 \pmod{p}$  but  $n^{2^{k-1}} \not\equiv 1 \pmod{p}$ , so that  $a$  is a quadratic non-residue modulo  $p$ , which means (5) has no solution. At this stage of the algorithm, we start a loop. We set  $b \equiv c^{2^{k-k'-1}} \pmod{p}$ , and then set  $r' \equiv br' \pmod{p}$ ,  $c' \equiv b^2 \pmod{p}$ , and  $n' \equiv c'n \pmod{p}$ . By multiplying both sides of (6) by  $b^2$ , we see that

$$b^2 r^2 \equiv a n b^2 \pmod{p} \Rightarrow (r')^2 \equiv a n' \pmod{p}. \quad (9)$$

There is a purpose to this construction:  $c'$  has order exactly equal to  $2^{k'}$ . To see this, observe that

$$(c')^{2^{k'}} \equiv (b^2)^{2^{k'}} \pmod{p} \equiv \left( (c^{2^{k-k'-1}})^2 \right)^{2^{k'}} \pmod{p} \equiv (c^{2^{k-k'-1}})^{2^{k'+1}} \pmod{p} \equiv c^{2^{k-k'-1+k'+1}} \pmod{p} \equiv 1 \pmod{p},$$

where the last step follows from (7). For  $l' < k'$  we would have

$$(c')^{2^{l'}} \equiv (b^2)^{2^{l'}} \pmod{p} \equiv \left( (c^{2^{k-k'-1}})^2 \right)^{2^{l'}} \pmod{p} \equiv (c^{2^{k-k'-1}})^{2^{l'+1}} \pmod{p} \equiv c^{2^{k-k'-1+l'+1}} \pmod{p} \not\equiv 1 \pmod{p},$$

since  $k - k' + l' = k - (k' - l') < k$ , and the order of  $c$  is exactly  $2^k$ . Now since  $n \not\equiv 1 \pmod{p}$  in the current case, we deduce that  $k' > 0$ . This is because if  $k' = 0$ , then

$$b \equiv c^{2^{k-1}} \pmod{p} \equiv -1 \pmod{p},$$

so

$$r' \equiv br' \pmod{p} \equiv -r' \pmod{p} \Rightarrow (r')^2 \equiv r'^2 \pmod{p} \equiv a n \pmod{p},$$

and the solution  $x \equiv \pm r' \pmod{p}$  corresponds to the case  $n \equiv 1 \pmod{p}$ . Now modulo  $p$ , each of  $n$  and  $c'$  has order  $2^{k'}$ . Hence by **Theorem 4** we see that the order of  $n'$  is  $2^{k''}$ , where  $k'' < k'$ . If  $k'' = 0$ , then

$$(n')^{2^0} = n' \equiv 1 \pmod{p},$$

and we deduce from (9) that it suffices to take  $x \equiv \pm r' \pmod{p}$ , for then

$$(r')^2 \equiv an' \pmod{p} \equiv a \pmod{p}.$$

If  $n' \not\equiv 1 \pmod{p}$ , then  $k'' > 0^1$ , and the situation is analogous to the one when the loop started. The only difference here is that  $c$  of order  $2^k$  has been replaced by  $c'$  of order  $2^{k'}$ , and  $n$  of order  $2^{k'}$  has been replaced by  $n'$  of order  $2^{k''}$ , whereas  $r$  has been replaced by  $r'$ , and correspondingly, (6) has been replaced by (9). Since  $k'' < k'$ , we have made progress, and after a finite number of executions of the loop, we shall eventually arrive at a set of these variables for which  $n \equiv 1 \pmod{p}$ , in which case  $x \equiv \pm r \pmod{p}$  is the desired solution.

## 4 An Example

We conclude this article with an illustration of how the algorithm works, using a numerical example. Suppose we wish to solve the congruence  $x^2 \equiv 10 \pmod{13}$ . We see that  $p - 1 = 12 = 2^2 \cdot 3$ , so  $k = 2$  and  $m = 3$ . Then

$$r \equiv 10^{\frac{3+1}{2}} \pmod{13} \equiv 100 \pmod{13} \equiv 9 \pmod{13},$$

and

$$n \equiv 10^3 \pmod{13} \equiv 12 \pmod{13} \equiv -1 \pmod{13}. \quad (10)$$

Since  $-1 \not\equiv 1 \pmod{13}$ , we need to find a quadratic non-residue  $z$  modulo 13. We notice that

$$2^{\frac{13-1}{2}} = 64 \equiv -1 \pmod{13},$$

so 2 is a quadratic non-residue modulo 13. Let  $z = 2$ , and then

$$c \equiv 2^3 \pmod{13} \equiv 8 \pmod{13}.$$

We now wish to determine the order of  $n$ . It is easy to see from (10) that  $n^2 \equiv 1 \pmod{13}$ , so the order of  $n$  is  $2^1 \Rightarrow k' = 1$ . We now start our loop. We set

$$b \equiv 8^{2^{2-1-1}} \pmod{13} \equiv 8 \pmod{13}.$$

Then

$$\begin{aligned} r' &\equiv br \pmod{13} \equiv 72 \pmod{13} \equiv 7 \pmod{13}, \\ c' &\equiv b^2 \pmod{13} \equiv 64 \pmod{13} \equiv -1 \pmod{13}, \\ n' &\equiv c'n \pmod{13} \equiv 1 \pmod{13}. \end{aligned}$$

At this point we see that  $n' \equiv 1 \pmod{13}$ , so we stop the loop, and deduce that  $x \equiv \pm r' \pmod{13} \equiv \pm 7 \pmod{13}$  are the two solutions to the congruence  $x^2 \equiv 10 \pmod{13}$ . It is easy to check that  $x^2 \equiv (\pm 7)^2 \pmod{13} \equiv 49 \pmod{13} \equiv 10 \pmod{13}$ .

---

<sup>1</sup>The text here says  $k'' > 1$  but I believe there is a typographical error, though I could very likely be wrong.