DAVE4MATH

Tonelli-Shanks Algorithm (by Example)

Last updated: January 23, 2021, Published: September 18, 2020 by Dave

(Dave)—Okay, so you understand how to check if a quadratic congruence is solvable, but how do you find the solutions? In this article, I cover the Tonelli-Shanks algorithm by working through several examples. I also give a complete solution to a general quadratic congruence equation.

CONTENTS

Solving quadratic congruence equations using a pseudo-random (Tonelli-Shanks) algorithm is discussed. We give several examples and many workable exercises.

Introduction to Tonelli-Shanks Algorithm

The Tonell-Shanks algorithm (sometimes called the RESSOL algorithm) is used within modular arithmetic where a is a quadratic residue (mod p), and p is an odd prime. Tonelli–Shanks cannot be used for composite moduli. Note that, finding square roots modulo composite numbers is a computational problem equivalent to integer factorization.

Theorem. (***Shanks)*** Let p be an odd prime and assume $(a, p) = 1$. Let x be a solution to $x^2 \equiv a \pmod{p}$ and let n and k be integers such that $p - 1 = 2^n k$ where $n \geq 1$ and k is odd, and let q be a quadratic nonresidue modulo p. Then x can be found by repeating the following loop:

(1) Set $t = a^{(k+1)/2} \pmod{p}$ and find the least i such that $r^{2^i} \equiv 1 \pmod{p}$ where $r = a^k \pmod{p}$.

(2) If $i = 0$ then the solutions are $x \equiv \pm t \pmod{p}$ else set $u \equiv q^{k(2^{n-i-1})} \pmod{p}$ and goto (i) and replace t by tu and r by ru^2.

Examples of the Tonelli-Shanks Algorithm

We solve three examples illustrating the use of the Tonelli-Shanks Algorithm.

Example. Solve the quadratic congruence $x^2 \equiv 29 \pmod{53}$.

Solution. First we find $53-1=52=2^2(13)$ and so we set $n=2$ and $k=13$. Next we find the a quadratic nonresidue. Since $\left(\frac{2}{53}\right)=-1$, we use $q=2$. With $a=29$, $q=2$, $n=2$, and $k=13$ we perform Shanks algorithm.

Loop 1: We find $t=29^7 \equiv 17 \pmod{53}$ and $r=29^{13} \equiv 52 \pmod{53}$. Next we find i:

i	52^{2^i}
0	$52^{2^0} \equiv 52 \pmod{53}$
1	$52^{2^1} \equiv 1 \pmod{53}$

Since $i \neq 0$ we find $u=2^{13(2^{2-1-1})} \equiv 30 \pmod{53}$.

Loop 2: We find $t=17(30) \equiv 33 \pmod{53}$ and $r=52(30)^2 \equiv 1 \pmod{53}$. Next we find i:

i	1^{2^i}
0	$1^{2^0} \equiv 1 \pmod{53}$

Since $i=0$, we find $x=\pm 33 \pmod{53}$. Therefore the solutions are $x \equiv 20, 33 \pmod{53}$.

Example. Solve the quadratic congruence $x^2 \equiv 37 \pmod{137}$.

Solution. We let $a=37$. Since $137-1=2^3 17$ we let $n=3$, $k=17$. Also, since $\left(\frac{3}{137}\right)=-1$ we let $q=3$ and perform Shanks algorithm.

Loop 1: We find $t=37^9 \equiv 37 \pmod{137}$ and $r=37^{17} \equiv 37 \pmod{137}$. Next we find i:

i	37^{2^i}
0	$37^{2^0} \equiv 37 \pmod{137}$
1	$37^{2^1} \equiv 136 \pmod{137}$
2	$37^{2^2} \equiv 1 \pmod{137}$

Since $i \neq 0$ we find $u = 127 \pmod{137}$.

Loop 2: We find $t = 37(127) \equiv 41 \pmod{137}$ and $r = 37(127)^2 \equiv 1 \pmod{137}$. Next we find i:

i	1^{2^i}
0	$1^{2^0} \equiv 1 \pmod{137}$

Since $i = 0$ we find $x \equiv \pm 41 \pmod{137}$. Therefore the solutions are $x \equiv 41, 96 \pmod{137}$.

Another Example of the Tonelli-Shanks Algorithm

Example. Solve the quadratic congruence $x^2 \equiv 11 \pmod{257}$.

Solution. We let $a = 11$. Since $257 - 1 = 256 = 2^8(1)$ we let $n = 8$, $k = 1$. Also, since $\left(\frac{5}{257}\right) = -1$ we let $q = 5$ and perform Shanks algorithm.

(Loop 1) We find $t = 11^1 \equiv 11 \pmod{257}$ and $r = 11^1 \equiv 11 \pmod{257}$. Next we find i:

i	11^{2^i}
0	$11^{2^0} \equiv 11 \pmod{257}$
1	$11^{2^1} \equiv 121 \pmod{257}$
2	$11^{2^2} \equiv 249 \pmod{257}$
3	$11^{2^3} \equiv 64 \pmod{257}$
4	$11^{2^4} \equiv 241 \pmod{257}$
5	$11^{2^5} \equiv 256 \pmod{257}$
6	$11^{2^6} \equiv 1 \pmod{257}$

Since $i \neq 0$ we find $u = 5^{1(2^{8-6-1})} \equiv 25 \pmod{257}$.

(Loop 2) We find $t = 11(25) \equiv 18 \pmod{257}$ and $r = 11(25)^2 \equiv 193 \pmod{257}$. Next we find i:

i	193^{2^i}
0	$193^{2^0} \equiv 193 \pmod{257}$
1	$193^{2^1} \equiv 241 \pmod{257}$
2	$193^{2^2} \equiv 256 \pmod{257}$
3	$193^{2^3} \equiv 1 \pmod{257}$

Since $i \neq 0$ we find $u = 5^{1(2^{8-3-1})} \equiv 225 \pmod{257}$.

(Loop 3) We find $t = 18(225) \equiv 195 \pmod{257}$ and $r = 193(225)^2 \equiv 256 \pmod{257}$. Next we find i:

i	256^{2^i}
0	$256^{2^0} \equiv 256 \pmod{257}$
1	$256^{2^1} \equiv 1 \pmod{257}$

Since $i \neq 0$ we find $u = 5^{1(2^{8-1-1})} \equiv 16 \pmod{257}$.

(Loop 4) We find $t = 195(16) \equiv 36 \pmod{257}$ and $r = 256(16)^2 \equiv 1 \pmod{257}$. Next we find i:

i	1^{2^i}
0	$1^{2^0} \equiv 1 \pmod{257}$

Solving Quadratic Congruences

Example. Find all solutions to the quadratic congruence equation

$$f(x) = 2x^2 + 10x + 1 \equiv 0 \pmod{1429530274918301}.$$

Solution. The first step in our method is to find the unique factorization of the mod namely,

$$m = 1429530274918301 = 101^3 193^4.$$

Now we divide this problem into solving both of the following equations.

$$2x^2 + 10x + 1 \equiv 0 \pmod{101}$$

$$2x^2 + 10x + 1 \equiv 0 \pmod{193}$$

First we solve the first by making the linear change of variables $y = 4x + 10$ and $d = 92$ because solving $(???)$ is equivalent to solving $y^2 \equiv 92 \pmod{101}$ since

$$\begin{aligned} y^2 - 92 &= (4x + 10)^2 - 92 \\ &= 100 + 80x + 16x^2 - 92 \\ &\equiv 2x^2 + 10x + 1 \pmod{101} \\ &\equiv 0 \pmod{101}. \end{aligned}$$

To determine if $y^2 \equiv 92 \pmod{101}$ is solvable we compute the Legendre symbol $\left(\frac{92}{101}\right)$ by first factoring $92 = 2^2 23$ and then we apply the law of quadratic reciprocity to find,

$$\begin{aligned} \left(\frac{92}{101}\right) &= \left(\frac{2^2}{101}\right)\left(\frac{23}{101}\right) \\ &= \left(\frac{23}{101}\right) \\ &= \left(\frac{101}{23}\right) \\ &= \left(\frac{9}{23}\right) \\ &= 1. \end{aligned}$$

Use the Tonelli-Shanks algorithm to solve $y^2 \equiv 92 \pmod{101}$

So now we use Shank's algorithm to solve $y^2 \equiv 92 \pmod{101}$. First we find $101 - 1 = 100 = 2^2(25)$ and so we set $n = 2$ and $k = 25$. With $a = 92$, $n = 2$, and $k = 25$ we perform Shanks algorithm and find $t \equiv 92^{13} \equiv 71 \pmod{101}$ and $r \equiv 92^{25} \equiv 1 \pmod{101}$. Therefore, Shank's algorithm terminates during the first loop and the solutions are $y = \pm 71$.

So we need to solve

$$71 \equiv 4x + 10 \pmod{101}$$

and

$$-71 \equiv 4x + 10 \pmod{101}.$$

For the first congruence equation we obtain $x \equiv 91 \pmod{101}$ and for the second we obtain $x \equiv 5 \pmod{101}$. Therefore the two solutions of the quadratic congruence $2x^2 + 10x + 1 \equiv 0 \pmod{101}$ are $x \equiv 91 \pmod{101}$ and $x \equiv 5 \pmod{101}$.

Next we solve the second by making the linear change of variables $y = 4x + 10$ and $d = 92$ because solving $2x^2 + 10x + 1 \equiv 0 \pmod{193}$ is equivalent to solving $y^2 \equiv 92 \pmod{193}$. To determine if this equation is solvable we compute the Legendre symbol $\left(\frac{92}{193}\right)$ by first factoring $92 = 2^2 23$. Then

$$\begin{aligned}\left(\frac{92}{193}\right) &= \left(\frac{2^2}{193}\right)\left(\frac{23}{193}\right) \\ &= \left(\frac{23}{193}\right) \\ &= \left(\frac{193}{23}\right) \\ &= \left(\frac{9}{23}\right) \\ &= 1\end{aligned}$$

Therefore, $y^2 \equiv 92 \pmod{193}$ is solvable.

Use the Tonelli-Shanks algorithm to solve $y^2 \equiv 92 \pmod{193}$

Now we use Shank's algorithm to solve $y^2 \equiv 92 \pmod{193}$. First we find $193 - 1 = 192 = 2^6(3)$ and so we set $n = 6$ and $k = 3$. Next we find a quadratic nonresidue of 193 namely $q = 5$ since $\left(\frac{5}{193}\right) = -1$. Now with $a = 92$, $q = 5$, $n = 6$, and $k = 3$ we perform Shank's algorithm

(Loop 1) We find $t = 92^2 \equiv 165 \pmod{193}$ and $r = 92^3 \equiv 126 \pmod{193}$. Next we find i:

i	126^{2^i}
0	$126^{2^0} \equiv 126 \pmod{193}$
1	$126^{2^1} \equiv 50 \pmod{193}$
2	$126^{2^2} \equiv 184 \pmod{193}$
3	$126^{2^3} \equiv 81 \pmod{193}$
4	$126^{2^4} \equiv 192 \pmod{193}$
5	$126^{2^5} \equiv 1 \pmod{193}$

Since $i \neq 0$ we find $u = 5^{3(2^{6-5-1})} \equiv 125 \pmod{193}$.

(Loop 2) We find $t = 165(125) \equiv 167 \pmod{193}$ and $r = 126(125)^2 \equiv 150 \pmod{193}$. Next we find i:

i	150^{2^i}
0	$150^{2^0} \equiv 150 \pmod{193}$
1	$150^{2^1} \equiv 112 \pmod{193}$
2	$150^{2^2} \equiv 192 \pmod{193}$
3	$150^{2^3} \equiv 1 \pmod{193}$

Since $i \neq 0$ we find $u = 5^{3(2^{6-3-1})} \equiv 64 \pmod{193}$.

(Loop 3) We find $t = 167(64) \equiv 73 \pmod{193}$ and $r = 150(64)^2 \equiv 81 \pmod{193}$. Next we find i:

i	81^{2^i}
0	$81^{2^0} \equiv 81 \pmod{193}$
1	$81^{2^1} \equiv 192 \pmod{193}$
2	$81^{2^2} \equiv 1 \pmod{193}$

Since $i \neq 0$ we find $u = 5^{3(2^{6-2-1})} \equiv 43 \pmod{193}$.

(Loop 4) We find $t = 73(43) \equiv 51 \pmod{193}$ and $r = 81(43)^2 \equiv 1 \pmod{193}$.

The Tonelli-Shanks algorithm terminates

Therefore, the Tonelli-Shanks algorithm terminates and the solutions are $y = \pm 51$. So we need to solve $51 \equiv 4x + 10 \pmod{193}$ and $-51 \equiv 4x + 10 \pmod{193}$. For the first congruence equation we obtain $x \equiv 155 \pmod{193}$ and for the second we obtain $x \equiv 33 \pmod{193}$. Therefore the two solutions of the quadratic congruence $2x^2 + 10x + 1 \equiv 0 \pmod{193}$ are $x \equiv 155 \pmod{193}$ and $x \equiv 33 \pmod{193}$.

Lift our solutions

Next we will use Hensel's lifting theorem to lift to solutions modulo 101^3 and 193^4. Thus we compute $f'(x) = 4x + 10$ and we notice that

$$\begin{aligned} f'(5) &\equiv 30 \neq 0 \pmod{101} & f'(91) &\equiv 71 \neq 0 \pmod{101} \\ f'(33) &\equiv 142 \neq 0 \pmod{193} & f'(155) &\equiv 51 \neq 0 \pmod{193} \end{aligned}$$

Since these values of the derivative are nonzero we know each of these four solutions lift (uniquely) up to the necessary powers. To do so we compute the inverses of each, namely,

$$\begin{aligned} 30u_1 &\equiv 1 \pmod{101} \Rightarrow u_1 = 64 \\ 71u_2 &\equiv 1 \pmod{101} \Rightarrow u_2 = 37 \\ 142u_3 &\equiv 1 \pmod{193} \Rightarrow u_3 = 140 \\ 51u_4 &\equiv 1 \pmod{193} \Rightarrow u_4 = 53 \end{aligned}$$

Now using the inverses we just computed we can lift our 4 solutions as follows.

k	$x_k = x_{k-1} - f(x_{k-1})64$
1	$x_1 \equiv 5 \pmod{101^1}$
2	$x_2 = 5 - f(5)64 \equiv 3742 \pmod{101^2}$
3	$x_3 = 3742 - f(3742)64 \equiv 64948 \pmod{101^3}$

k	$x_k = x_{k-1} - f(x_{k-1})37$
1	$x_1 \equiv 91 \pmod{101^1}$
2	$x_2 = 6454 - f(6454)37 \equiv 6454 \pmod{101^2}$
3	$x_3 = 6454 - f(6454)37 \equiv 965348 \pmod{101^3}$

k	$x_k = x_{k-1} - f(x_{k-1})140$
1	$x_1 \equiv 33 \pmod{193^1}$
2	$x_2 = 33 - f(33)140 \equiv 21263 \pmod{193^2}$
3	$x_3 = 21263 - f(21263)140 \equiv 6055601 \pmod{193^3}$
4	$x_4 = 6055601 - f(6055601)140 \equiv 811229985 \pmod{193^4}$

k	$x_k = x_{k-1} - f(x_{k-1})53$
1	$x_1 \equiv 155 \pmod{193^1}$
2	$x_2 = 155 - f(155)53 \equiv 15981 \pmod{193^2}$
3	$x_3 = 15981 - f(15981)53 \equiv 1133451 \pmod{193^3}$
4	$x_4 = 1133451 - f(1133451)53 \equiv 576258011 \pmod{193^4}$

To recap, $2x^2 + 10x + 1 \equiv 0 \pmod{101^3}$ has solutions 64948 and 965348 and $2x^2 + 10x + 1 \equiv 0 \pmod{193^4}$ has solutions 811229985 and 576258011.

The four solutions

Finally, to solve our originally congruence equation we use the Chinese Remainder Theorem to solve the 4 linear systems:

$$(1) \quad \begin{cases} x \equiv 64948 \pmod{101^3} \\ x \equiv 811229985 \pmod{193^4} \end{cases} \qquad (2) \quad \begin{cases} x \equiv 64948 \pmod{101^3} \\ x \equiv 576258011 \pmod{193^4} \end{cases}$$

$$(3) \quad \begin{cases} x \equiv 965348 \pmod{101^3} \\ x \equiv 811229985 \pmod{193^4} \end{cases} \qquad (4) \quad \begin{cases} x \equiv 965348 \pmod{101^3} \\ x \equiv 576258011 \pmod{193^4} \end{cases}$$

We use the following tables to construct the four solutions.

i	n_i	a_i	$\bar{n}_i$	u_i
1	101^3	64948	193^4	$193^4 u_1 \equiv 1 \pmod{101^3} \implies u_1 = 970433$
2	193^4	811229985	101^3	$101^3 u_2 \equiv 1 \pmod{193^4} \implies u_2 = 80623169$

So a solution to (1) is

$$\begin{aligned} x_1 &= (64948)\left(193^4\right)(970433) + (811229985)\left(101^3\right)(80623169) \\ &\equiv 1193121168121899 \pmod{m}. \end{aligned}$$

i	n_i	a_i	$\bar{n}_i$	u_i
1	101^3	64948	193^4	$193^4 u_1 \equiv 1 \pmod{101^3} \Longrightarrow u_1 = 970433$
2	193^4	576258011	101^3	$101^3 u_2 \equiv 1 \pmod{193^4} \Longrightarrow u_2 = 80623169$

So the solution to (2) is

$$\begin{aligned} x_2 &= (64948)\left(193^4\right)(970433)(576258011)\left(101^3\right)(80623169) \\ &\equiv 1386887794953578 \pmod{m}. \end{aligned}$$

i	n_i	a_i	$\bar{n}_i$	u_i
1	101^3	965348	193^4	$193^4 u_1 \equiv 1 \pmod{101^3} \Longrightarrow u_1 = 970433$
2	193^4	811229985	101^3	$101^3 u_2 \equiv 1 \pmod{193^4} \Longrightarrow u_2 = 80623169$

So the solution to (3) is

$$\begin{aligned} x_3 &= (965348)\left(193^4\right)(970433) + (811229985)\left(101^3\right)(80623169) \\ &\equiv 42642479964718 \pmod{m}. \end{aligned}$$

i	n_i	a_i	$\bar{n}_i$	u_i
1	101^3	965348	193^4	$193^4 u_1 \equiv 1 \pmod{101^3} \Longrightarrow u_1 = 970433$
2	193^4	576258011	101^3	$101^3 u_2 \equiv 1 \pmod{193^4} \Longrightarrow u_2 = 80623169$

So the solution to (4) is

$$\begin{aligned} x_4 &= (965348)\left(193^4\right)(970433) + (576258011)\left(101^3\right)(80623169) \\ &\equiv 236409106796397 \pmod{m}. \end{aligned}$$

Therefore, the four and only four solutions are 1193121168121899, 1386887794953578, 42642479964718, and 236409106796397.

Exercises on Tonelli-Shanks Algorithm

Exercise. Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 6 \pmod{37}$.

Exercise. Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 21 \pmod{37}$.

Exercise. Rewrite an equivalent quadratic congruence (in standard form) and test w er (or not) Shank's Algorithm applies: $3x^2 - 2x + 7 \equiv 0 \pmod{23}$.

Exercise. Solve $x^2 \equiv 25 \pmod{127}$.

Exercise. Solve $x^2 \equiv 35 \pmod{127}$.

Exercise. Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 6 \pmod{37}$.

Exercise. Determine whether (or not) Shank's Algorithm applies to $x^2 \equiv 21 \pmod{37}$.

Exercise. Rewrite an equivalent quadratic congruence (in standard form) and test whether (or not) Shank's Algorithm applies: $3x^2 - 2x + 7 \equiv 0 \pmod{23}$.

Exercise. Solve $x^2 \equiv 25 \pmod{127}$. [Hint: You may use Shank's Algorithm, but you do not need to.]

Exercise. Solve $x^2 \equiv 35 \pmod{127}$ using Shank's Algorithm.

Recommended Articles

Quadratic Congruences and Quadratic Residues

Euler’s Totient Function and Euler’s Theorem

Fermat's Theorem (and Wilson's Theorem)

Chinese Remainder Theorem (The Definitive Guide)

Applications of Congruence (in Number Theory)

Polynomial Congruences with Hensel's Lifting Theorem

Linear Congruences and Their Solvability

Congruence Theorems (and Their Proofs)

Diophantine Equations (of the Linear Kind)

Fundamental Theorem of Arithmetic

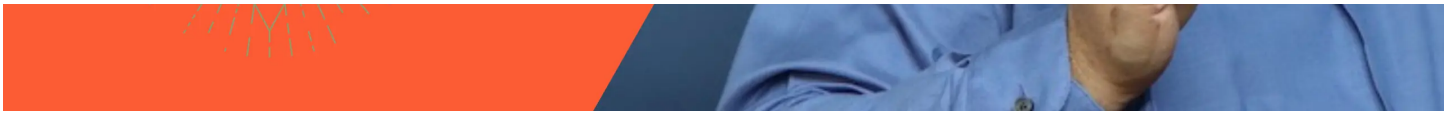
Euclidean Algorithm (by Example)

Greatest Common Divisors (and Their Importance) [Video]

David Smith (Dave) has a B.S. and M.S. in Mathematics and has enjoyed teaching precalculus, calculus, linear algebra, and number theory at both the junior college and university levels for over 20 years. David is the founder and CEO of Dave4Math.

LaTeX Typesetting: Trusted, Fast, and Accurate

LaTeX Graphics: Custom Graphics Using TikZ and PGFPlots



SERVICES

Math Help

Math Services

Testimonials

Math Solutions

Math Videos

LaTeX Typesetting

LaTeX Graphics

ONLINE COURSES

Precalculus

MATH BLOG

DAVE4MATH