Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **4** (2010), 23–31. doi:10.2298/AADM100201012K

NUMERICAL ANALYSIS MEETS NUMBER THEORY: USING ROOTFINDING METHODS TO CALCULATE INVERSES MOD p^n

Michael P. Knapp, Christos Xenophontos

We show how classical rootfinding methods from numerical analysis can be used to calculate inverses of units modulo prime powers.

1. INTRODUCTION

In this article we explore a very interesting application of tools from numerical analysis to number theory. As the title suggests, we will see how one can use classical rootfinding methods, such as Newton's method, to calculate the reciprocal of an integer modulo p^n, where p is a prime number. We first encountered this idea in [**3**], where Newton's method was used to find the reciprocal of a finite segment p-adic number (also referred to as Hensel code; see [**3**] for more details). In our experience, many people who specialize in either number theory or numerical analysis do not study the other subject, and so we have attempted to keep our exposition at a uniformly low level so that specialists in either field may benefit from this article.

We define fractions modulo p^n in the usual way as follows. If a, b and α are integers and a is not divisible by p, then we say that

$$\alpha \equiv \frac{b}{a} \pmod{p^n} \qquad \text{if} \qquad a\alpha \equiv b \pmod{p^n}.$$

Using this definition, the reciprocal $\frac{1}{a}$ of an integer a modulo p^n is a solution of the congruence $ax \equiv 1 \pmod{p^n}$. In other words, it is an inverse of a modulo p^n.

2000 Mathematics Subject Classification. 11A07 (65-01).
Keywords and Phrases. Newton's method, inverses modulo p^n, secant method.

The idea of using Newton's method to perform division (or calculate inverses) dates back to the early days of computing, since one can actually approximate the reciprocal of a number by performing only the operations of multiplication and addition. The idea behind iterative rootfinding methods such as Newton's method is as follows. Suppose that we have a function $f(x)$ for which we wish to find a zero in an interval $[a, b]$. To accomplish this, let $x_0 \in [a, b]$ be an initial guess for the zero, and let $g(x)$ be an iteration function. Then we calculate further approximations through the formula

$$x_{i+1} = g(x_i), \quad i = 0, 1, \ldots \tag{1}$$

If the initial guess x_0 and the iteration function $g(x)$ are suitably chosen, then the sequence $x_0, x_1, x_2, \ldots$ should converge to a zero of $f(x)$ in $[a, b]$.

If this does in fact occur, then we can talk about the rate at which the sequence converges to a zero of $f(x)$. Roughly speaking, if the rate of convergence of a method is m (i.e. the method converges with order m), then after each iteration the number of correct significant digits in the approximation increases by a factor of approximately m. For example, if our approximation converges quadratically (i.e. with order 2), then the number of correct significant digits approximately doubles with each iteration.

Now let us see what this has to do with congruences modulo p^n. In this situation, the role of significant digits will be played by smaller powers of p. We will start with an inverse of a modulo p, and then find inverses of a modulo higher powers of p until we have an inverse modulo p^n. The connection between digits and powers of p can be found by looking at the base p representation of numbers. It is well-known that any positive integer α has a base p representation

$$\alpha = c_0 + c_1 p + c_2 p^2 + \cdots + c_k p^k,$$

where $0 \leq c_i \leq p-1$ for each i. Each coefficient c_i is a digit in the base p representation of α. To find a number which is congruent to α modulo p^r, we can simply truncate the base p expansion of α after the first r digits. Thus, if $r < n$ then we may think of an inverse of a modulo p^r as giving the correct first r digits of an inverse of a modulo p^n.

We note here that our Theorems 1, 3 and 4 ahead are not truly original. In fact, they are simple consequences of more powerful theorems about iterative methods. However, we feel that our proofs are worthwhile because they are quite simple and avoid any heavy machinery.

2. NEWTON'S METHOD (FOR DIVISION MOD p^n)

The iteration function for Newton's method is $g(x) = x - f(x)/f'(x)$, whence equation (1) becomes

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)} \ , \quad i = 0, 1, \ldots \tag{2}$$

Under suitable assumptions on f, f' and x_0 (see for example Theorem 3.2 on page 100 of [**1**]), the above iteration converges to a zero of $f(x)$ in $[a, b]$ at a *quadratic* rate. So to calculate $\frac{1}{a}$, we let $f(x) = \frac{1}{x} - a$, and solve $f(x) = 0$ using Newton's Method. In this case iteration (2) becomes

$$x_{i+1} = x_i(2 - ax_i) \ , \ \ i = 0, 1, \ldots \tag{3}$$

Like Newton's method for real numbers, we can show that Newton's method also converges quadratically for congruences. This is proven in the following theorem. Although we're using different language, this is essentially the same as the main theorem of [**3**]. We believe that our proof is simpler, however.

Theorem 1. *Let $\alpha > 0$ and suppose that x_i is an inverse of a modulo p^α. Then x_{i+1} given by* (3) *is an inverse of a modulo $p^{2\alpha}$.*

Proof. To prove this, we know that $ax_i \equiv 1 \pmod{p^\alpha}$, and therefore can write $ax_i = sp^\alpha + 1$ for some integer s. Then we have

$$\begin{aligned} ax_{i+1} &= ax_i(2 - ax_i) \\ &= -s^2p^{2\alpha} + 1 \\ &\equiv 1 \pmod{p^{2\alpha}}. \end{aligned}$$

Hence x_{i+1} is an inverse of a modulo $p^{2\alpha}$, as desired. □

So if we can find an inverse of a modulo p to use as an initial guess, then we can use Newton's method to find inverses of a modulo p^2, p^4, p^8 and so on. If the prime p is small, then we can often find an inverse of a modulo p by inspection. If p is larger, then we can use Fermat's Little Theorem to find our initial guess.

Theorem 2. (Fermat's Little Theorem) *Suppose that p is prime and that a is an integer not divisible by p. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

An easy consequence of this theorem is that if p does not divide a, then a^{p-2} is an inverse of a modulo p.

We can evaluate a^{p-2} modulo p by the technique of repeated squaring. For example, to find the inverse of 29 modulo 53, we need to evaluate 29^{51} modulo 53. To do this, we have

$$\begin{aligned} 29^1 &\equiv 29 \pmod{53} \\ 29^2 &\equiv 46 \pmod{53} \\ 29^4 \equiv 46^2 &\equiv 49 \pmod{53} \\ 29^8 \equiv 49^2 &\equiv 16 \pmod{53} \\ 29^{16} \equiv 16^2 &\equiv 44 \pmod{53} \\ 29^{32} \equiv 44^2 &\equiv 28 \pmod{53}. \end{aligned}$$

Thus we obtain

$$29^{51} = 29^{32} \cdot 29^{16} \cdot 29^2 \cdot 29^1 \equiv (28)(44)(46)(29) \equiv 11 \pmod{53},$$

and so $\frac{1}{29} \equiv 11 \pmod{53}$.

Let us now illustrate the use of Newton's method in the context of the present paper via an example.

EXAMPLE 1. Let $p = 5$, $a = 3$ and $n = 8$. We wish to find an integer congruent to $\frac{1}{3}$ modulo 5^8 using the Newton iteration (3). As our initial guess, we choose $x_0 = 2$ since $3(2) \equiv 1 \pmod 5$ and so $2 \equiv \frac{1}{3} \pmod 5$. Then we have from (3) that

$$x_1 = 2\,(2 - 3 \cdot 2) = -8 \equiv 17 = 2 + 3(5) \pmod{5^2}.$$

Note that $3(17) = 51 \equiv 1 \pmod{5^2}$, and so $17 \equiv \frac{1}{3} \pmod{5^2}$ as indicated by Theorem 1. Iterating twice more gives us

$$x_2 \equiv 417 = 2 + 3(5) + 1(5)^2 + 3(5)^3 \pmod{5^4}$$
$$x_3 \equiv 260417 = 2 + 3(5) + 1(5)^2 + 3(5)^3 + 1(5)^4 + 3(5)^5 + 1(5)^6 + 3(5)^7 \pmod{5^8},$$

and so we see that $260417 \equiv \frac{1}{3} \pmod{5^8}$.

3. THE SECANT METHOD (FOR DIVISION MOD p^n)

Another well-known rootfinding method is the secant method, whose iteration is given by

$$x_{i+1} = x_i - \frac{f(x_i)(x_i - x_{i-1})}{f(x_i) - f(x_{i-1})} \quad , \quad i = 1, 2, \ldots \tag{4}$$

Note that we now need *two* initial guesses x_0 and x_1, but we no longer need the derivative[1] of $f(x)$. Since "there is no such thing as a free lunch", the trade-off is that the order of convergence drops down to the golden ratio $\phi = (1 + \sqrt{5})/2$. In fact, we will show that after each iteration, instead of doubling (like in Newton's method), the number of correct digits increases by a factor of approximately ϕ. For our function $f(x) = \frac{1}{x} - a$, equation (4) becomes

$$x_{i+1} = x_i + x_{i-1} - a x_i x_{i-1}. \tag{5}$$

To establish the rate of convergence when using the secant method for congruences we have the following theorem.

[1] This is important when the derivative of the function $f(x)$ is difficult to obtain; however, this is not the case here.

Theorem 3. *Suppose that* $x_{i-1} \equiv \frac{1}{a} \pmod{p^\alpha}$ *and that* $x_i \equiv \frac{1}{a} \pmod{p^\beta}$. *Then, with* x_{i+1} *given by* (5), *we have* $x_{i+1} \equiv \frac{1}{a} \pmod{p^{\alpha+\beta}}$.

Proof. To prove this, note that since we have $ax_{i-1} \equiv 1 \pmod{p^\alpha}$ and $ax_i \equiv 1 \pmod{p^\beta}$, there exist integers s and t such that

$$ax_{i-1} = sp^\alpha + 1 \qquad \text{and} \qquad ax_i = tp^\beta + 1.$$

Then we have

$$\begin{aligned} ax_{i+1} &= ax_i + ax_{i-1} - (ax_i)(ax_{i-1}) \\ &= -\mathrm{stp}^{\alpha+\beta} + 1 \\ &\equiv 1 \pmod{p^{\alpha+\beta}}, \end{aligned}$$

as desired. □

So if x_1 and x_2 are both inverses of a modulo p^1, we can show by induction that x_i is the inverse of a modulo p^{F_i}, where F_i is the i^{th} Fibonacci number. Since it is well-known that F_i gets closer and closer to $\phi^n/\sqrt{5}$ as n gets large, we find that the secant method has order of convergence ϕ.
Another way to see this is by introducing the errors

$$\varepsilon_{i+1} = |x_{i+1} - 1/a|, \varepsilon_i = |x_i - 1/a|, \varepsilon_{i-1} = |x_{i-1} - 1/a|.$$

Then (5) gives the relation

$$\varepsilon_{i+1} = |a|\varepsilon_i\varepsilon_{i-1}. \tag{6}$$

Assuming that the rate of convergence of the secant method is r, we have

$$\varepsilon_{i+1} \approx A\varepsilon_i^r \iff \varepsilon_i \approx A\varepsilon_{i-1}^r \iff \frac{\varepsilon_i^{1/r}}{A^{1/r}} \approx \varepsilon_{i-1}, \tag{7}$$

for some positive constant A. Thus, by (6) and (7) we get

$$\varepsilon_{i+1} \approx C\frac{1}{A^{1/r}}\varepsilon_i^{1/r}\varepsilon_i \approx B\varepsilon_i^{1+1/r},$$

where B, C are positive constants. Hence, $\varepsilon_i^{1+1/r} \approx \frac{A}{B}\varepsilon_i^r$, from which it follows that $1 + 1/r = r$, or equivalently that the order of convergence of the secant method is given by the positive root of the equation $r^2 - r - 1 = 0$, i.e. $r = \phi = (1+\sqrt{5})/2 \approx 1.6$.

It is worth noticing that although the general formula (4) for the iteration requires that our initial guesses x_0 and x_1 be different, this is not required in either formula (5) or Theorem 3. Thus we can take x_0 and x_1 to both be inverses of a modulo p, and in fact can even take them to be the same number. Let us illustrate the above ideas via an example.

EXAMPLE 2. Let $p = 7, a = 5$ and $n = 8$, i.e. we wish to find an integer congruent to $\frac{1}{5}$ modulo 7^8 using the iteration (5). We choose $x_0 = x_1 = 3$, since $5 \cdot 3 \equiv 1 \pmod 7$. We have from (5)

$$\begin{aligned}
x_2 &= 3 + 3 - 5 \cdot 3 \cdot 3 \equiv 10 = 3 + 1(7) \pmod{7^2} \\
x_3 &= 10 + 3 - 5 \cdot 10 \cdot 3 \equiv 206 = 3 + 1(7) + 4(7)^2 \pmod{7^3} \\
x_4 &\equiv 6723 = 3 + 1(7) + 4(7)^2 + 5(7)^3 + 2(7)^4 \pmod{7^5} \\
x_5 &\equiv 4611841 = \\
&= 3 + 1(7) + 4(7)^2 + 5(7)^3 + 2(7)^4 + 1(7)^5 + 4(7)^6 + 5(7)^7 \pmod{7^8}
\end{aligned}$$

and so we see that $4611841 \equiv \frac{1}{5} \pmod{7^8}$.

4. FIXED POINT ITERATION AND HIGH ORDER CONVERGENT METHODS

The general iteration formula (1) actually defines a larger class of iterative methods, called *fixed point* methods: instead of solving $f(x) = 0$ we solve $g(x) = x$ (for a suitably chosen $g(x)$). The advantage of this approach is that it can be easily generalized to higher dimensions and analyzed using a plethora of famous fixed point theorems. Newton's method is a special case of a fixed point iteration, as can be readily seen by equation (2). Under suitable assumptions on g (see Theorems 3.5 and 3.7 on pages 121–124 of [**1**]), iteration (1) converges to α for any initial guess x_0 sufficiently close to α, at a rate r such that

$$g(\alpha) = \alpha, \quad g'(\alpha) = g''(\alpha) = g'''(\alpha) = \cdots = g^{(r-1)}(\alpha) = 0 \quad \text{but} \quad g^{(r)}(\alpha) \neq 0. \tag{8}$$

With this in mind, one can construct iteration functions g such that (8) holds for some r, hence obtaining a method which converges at that rate.

In our case, Newton's method can be written as a fixed point iteration with $g(x) = x(2 - ax)$. Since we already know that this is a quadratically convergent method, we expect that $g\left(\frac{1}{a}\right) = \frac{1}{a}$, $g'\left(\frac{1}{a}\right) = 0$, and $g''\left(\frac{1}{a}\right) \neq 0$, and this is easily seen to be the case.

Now suppose we wanted to construct an iterative method for finding the zero of $f(x) = \frac{1}{x} - a$, with a higher convergence rate. To this end, define $u(x) = f(x)/f'(x)$ and $E_2(x) = x - u(x)$. Then, Newton's method corresponds to solving

$$x_{n+1} = E_2(x_n) \ , \ n = 0, 1, 2, \ldots$$

TRAUB [**5**] derived the following relation

$$E_{r+1}(x) = E_r(x) - \frac{u(x)}{r} E_r'(x) \ , \ r = 2, 3, \ldots \tag{9}$$

to produce a sequence of generalized iterative formulas, of order $r+1$, for solving non-linear equations, known as Schröder's method of the first kind [**4**].

In particular, if $f(x) = \frac{1}{x} - a$, then introducing $z = 1 - ax$ yields $x = (1-z)/a$ and $u = z(z-1)/a$, so that

$$E_2(x) = x(1 + (1 - az)) = \frac{1-z}{a}(1+z) = \frac{1-z^2}{a} = \frac{1-(1-ax)^2}{a}.$$

For arbitrary $r \geq 2$, assume that

$$E_r(x) = \frac{1-z^r}{a} = \frac{1-(1-ax)^r}{a}. \tag{10}$$

Then, applying (9) we obtain

$$E_{r+1} = \frac{1-z^r}{a} - \frac{z(z-1)}{a}z^{r-1} = \frac{1}{a}(1-z^{r+1}) = \frac{1}{a}\big(1-(1-ax)^{r+1}\big).$$

Therefore, we see that by induction, (10) holds true for arbitrary $r \geq 2$. As a result, an iterative method of order r (≥ 2) for finding an inverse of a modulo prime numbers is given by

$$x_{i+1} = E_r(x_i) \;\Leftrightarrow\; x_{i+1} = \frac{1}{a}\big(1-(1-ax_i)^r\big)\,,\; i = 0, 1, 2, \ldots \tag{11}$$

For example, for $r = 2$ we obtain (3) and for $r = 3$ we obtain

$$x_{i+1} = x_i[1 + (1 - ax_i)(2 - ax_i)]. \tag{12}$$

The following example illustrates the use of iteration (12).

Example 3. As in Example 1, let $p = 5$, $a = 3$ and $n = 8$. We wish to find an integer congruent to $\frac{1}{3}$ modulo 5^8 using the iteration (12). We expect that 2 iterations will suffice here, as opposed to 3 iterations which were needed in Example 1, since this method converges cubically. Indeed, with $x_0 = 2$,

$$x_1 = 2\,[1 + (1 - 3\cdot 2)(2 - 3\cdot 2)] = 42 \equiv 42 = 2 + 3(5) + 1(5)^2 \pmod{5^3}$$
$$x_2 = 42\,[1 + (1 - 3\cdot 42)(2 - 3\cdot 42)] = 651042 \equiv 651042 \pmod{5^9}.$$

Note that since 651042 is an inverse of 3 modulo 5^9, it is also an inverse of 3 modulo 5^8. Noting that $651042 \equiv 260417 \pmod{5^8}$, we see that

$$260417 = 2 + 3(5) + 1(5)^2 + 3(5)^3 + 1(5)^4 + 3(5)^5 + 1(5)^6 + 3(5)^7$$

is the smallest inverse of 3 modulo 5^8.

An assertion similar to Theorem 1, can be stated for the generalized method (11):

Theorem 4. *Let $\alpha > 0$ and suppose that x_i is an inverse of a modulo p^α. Then x_{i+1} given by* (11) *is an inverse of a modulo $p^{r\alpha}$.*

Proof. As before, we have $ax_i = sp^\alpha + 1$, for some integer s. Hence we have

$$\begin{aligned} ax_{i+1} &= aE_r(x_i) \\ &= 1 - (1 - ax_i)^r \\ &= 1 - (1 - sp^\alpha - 1)^r \\ &= 1 - (-1)^r s^r p^{\alpha r} \\ &\equiv 1 \pmod{p^{r\alpha}}. \end{aligned}$$

□

Our next example illustrates the use of iteration (11) with $r = 4$, i.e.

$$x_{i+1} = \frac{1}{a}\big(1 - (1 - ax_i)^4\big), \tag{13}$$

and compares the performance of all methods presented in this article.

EXAMPLE 4. Let $p = 2$, $a = 3$ and $n = 16$. We wish to find an integer congruent to $\frac{1}{3}$ modulo 2^{16} using iteration (13). As our initial guess we choose $x_0 = 1$, since $3 \cdot 1 \equiv 1 \pmod 2$. For comparison purposes, we will also show the answers obtained using iterations (3), (5) and (12) – for (5) we need a second initial guess, and we take $x_1 = 1$. Using iteration (13) we have

$$\begin{aligned} &x_1 \equiv 11 = 1 + (2) + (2)^3 \pmod{2^4} \\ &x_2 \equiv 43691 = 1 + (2) + (2)^3 + (2)^5 + (2)^7 + (2)^9 + (2)^{11} + (2)^{13} + (2)^{15} \pmod{2^{16}} \end{aligned}$$

and so we see that in just two iterations we obtain $43691 \equiv \frac{1}{3} \pmod{2^{16}}$.

For iteration (3) we obtain

$$x_1 \equiv 3 \pmod{2^2}, \quad x_2 \equiv 11 \pmod{2^4}, \quad x_3 \equiv 171 \pmod{2^8}, \quad x_4 \equiv 43691 \pmod{2^{16}},$$

while for iteration (5) we get

$$\begin{aligned} &x_2 \equiv 3 \pmod{2^2}, \quad x_3 \equiv 3 \pmod{2^3}, \quad x_4 \equiv 1 \pmod{2^5}, \quad x_5 \equiv 171 \pmod{2^8} \\ &x_6 \equiv 2731 \pmod{2^{13}}, \quad x_7 \equiv 699051 \pmod{2^{21}}, \end{aligned}$$

from which we obtain $43691 \equiv \dfrac{1}{3} \pmod{2^{16}}$, since $699051 \equiv 43691 \pmod{2^{16}}$.

Finally, for iteration (12), we have

$$x_1 \equiv 2 \pmod{2^3}, \quad x_2 \equiv 171 \pmod{2^9}, \quad x_3 \equiv 44739243 \pmod{2^{27}},$$

from which we get $43691 \equiv \dfrac{1}{3} \pmod{2^{16}}$, since $44739243 \equiv 43691 \pmod{2^{16}}$.

Therefore, we see that the secant method, which converges at the rate $(1+\sqrt{5})/2 \approx 1.6$, requires 7 iterations, the quadratically convergent Newton's method requires 4 iterations, while the cubically and quartically convergent iterations (12) and (13), require 3 and 2 iterations, respectively. These results demonstrate how the higher order methods can produce the desired inverse in a significantly smaller number of iterations.

Acknowledgements. We would like to thank ROBERT BENEDETTO and LISA OBERBROECKLING for some very helpful discussions about the rates of convergence of p-adic iterative methods.

We also thank the anonymous referee whose useful comments greatly improved Section 4.

The first author was partially supported by NSF grant DMS-0344082 during the preparation of this paper.

REFERENCES

1. J. Epperson: *An Introduction to Numerical Methods and Analysis.* Wiley and Sons, 2002.
2. E. V. Krishnamurthy: *Economical iterative and range transformation schemes for division.* IEEE Trans. Comput., **C-20** (1971), 470–472.
3. E. V. Krishnamurthy, V. K. Murthy: *Fast Iterative Division of p-adic Numbers.* IEEE Transactions on Computers, **32** (1983), 396–398.
4. E. Schröder: *Über unendlich viele Algorithmen zur Auflösung der Gleichunger.* Math. Annal., **2** (1870), 317–365.
5. J. F. Traub: *Iterative Methods for Solution of Equations.* Prentice Hall, Englewood Cliffs, New Jersey, 1964.

Mathematical Sciences Department,
Loyola University Maryland,
4501 N. Charles Street,
Baltimore, MD 21210
USA
E-mail: mpknapp@loyola.edu

Department of Mathematics and Statistics,
University of Cyprus,
P.O. Box 20537, 1678 Nicosia
Cyprus

(Received August 2, 2009)
(Revised February 1, 2010)