12. Beyond Newton-Raphson

Now let us consider the general problem of trying to find roots modulo m,

$$f(x) \equiv 0 \mod m.$$

Let $c_f(m)$ be the number of solutions modulo m.

Theorem 12.1. *The function*

$$c_f \colon \mathbb{N} \longrightarrow \mathbb{N},$$

is multiplicative.

Proof. Suppose that m and n are coprime. Suppose we are given a solution a to the equation

$$f(x) \equiv 0 \mod mn$$

Then

$$f(a) \equiv 0 \mod mn$$

so that

$$f(a) \equiv 0 \mod m \qquad \text{and} \qquad f(a) \equiv 0 \mod n.$$

Thus we get a solution to the equations

$$f(x) \equiv 0 \mod m \qquad \text{and} \qquad f(x) \equiv 0 \mod n.$$

Now suppose we are given solutions b and c to the equations

$$f(x) \equiv 0 \mod m \qquad \text{and} \qquad f(x) \equiv 0 \mod n.$$

It follows that

$$f(b) \equiv 0 \mod m \qquad \text{and} \qquad f(c) \equiv 0 \mod n.$$

By the Chinese remainder theorem there is a unique residue class a modulo mn such that

$$a \equiv b \mod m \qquad \text{and} \qquad a \equiv c \mod n.$$

More to the point, as

$$f(a) \equiv f(b) \equiv 0 \mod m \qquad \text{and} \qquad f(a) \equiv f(c) \equiv 0 \mod n$$

again by the Chinese remainder theorem,

$$f(a) \equiv 0 \mod mn,$$

so that a is a solution to the equation

$$f(x) \equiv 0 \mod mn.$$

It is then clear that

$$c_f(mn) = c_f(m)c_f(n).$$ □

By the fundamental theorem of arithmetic, it follows that if we want to solve the equation

$$f(x) \equiv 0 \mod m$$

it suffices to deal with the case that $m = p^e$, that is, we just have to solve

$$f(x) \equiv 0 \mod p^e,$$

where p is a prime and e is a natural number.

Note that if

$$f(a) \equiv 0 \mod p^e,$$

then certainly

$$f(a) \equiv 0 \mod p.$$

However we can't go quite go backwards. For example if a is a solution to the equation

$$f(x) \equiv 0 \mod p.$$

it need not be a solution to the equation

$$f(x) \equiv 0 \mod p^2.$$

From the first equation we know that $f(a)$ is a multiple of p but not necessarily a multiple of p^2. On the other hand, note that

$$a \qquad a+p \qquad a+2p \dots a+(p-2)p \qquad \text{and} \qquad a+(p-1)p,$$

are all different modulo p^2 and all equivalent to a modulo p. So we have to check to see which of these integers are solutions modulo p^2.

Fortunately there is a much more elegant and convenient way to proceed. The idea is to think of the problem of going from a solution modulo p^{e-1} to a solution modulo p^e as a problem of approximation.

The classic method of approximation proceeds as follows. Suppose you want to approximate the value of $\xi = \sqrt{2}$. This is a real number. Suppose we already have an approximation x_0, where we assume that the difference $h = \xi - x_0$ is relatively small. For example, $2.25 = 9/4$ is a perfect square, so that $x_0 = 3/2$ is a reasonable approximation to $\sqrt{2}$.

Introduce the function $f(x) = x^2$. Suppose that $f'(x_0) \neq 0$. Write down the Taylor series for $f(x)$ centred around x_0. We have

$$\begin{aligned} 0 &= f(\xi) \\ &= f(x_0) + hf'(x_0) + \frac{h^2}{2} f''(x_0) + \dots \\ &\simeq f(x_0) + hf'(x_0). \end{aligned}$$

Here we assume that the terms involving h^2, h^3 are small, as h is small. It follows that a good approximation $\hat{h}$ for h is given by solving

$$f(x_0) + \hat{h}f'(x_0) = 0.$$

This gives

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)},$$

the usual formula for Newton-Raphson approximation. If x_0 is close enough to ξ then x_1 will be closer to ξ.

We try the same idea to go from a solution modulo p^e to a solution modulo p^{e+1}. A polynomial has a very simple Taylor series that always ends with the term of order h^n, where n is the degree of f,

$$f(x_0 + h) = f(x_0) + f(x_0)h + \frac{f'(x_0)}{2}h^2 + \cdots + \frac{f^n(x_0)}{n!}h^n.$$

Consider a term of the form $c_j x^j$ in the polynomial $f(x)$. If we differentiate this k times then we have to multiply by

$$j(j-1)\dots(j-k+1).$$

This term then makes a contribution of

$$\frac{j(j-1)\dots(j-k+1)}{k!}c_j x_0^{j-k} = \binom{j}{k} c_j x_0^{j-k}.$$

In particular if c_j is an integer then this contribution is an integer. Thus if x_0 is an integer and $f(x) \in \mathbb{Z}[x]$ then the coefficients of the Taylor series expansion are integers.

Suppose that x_0 is a solution to the equation

$$f(x) \equiv 0 \mod p^e,$$

so that

$$f(x_0) \equiv 0 \mod p^e.$$

Now there are p residue classes modulo p^{e+1} that have residue modulo p^e, namely,

$$x_0, \qquad x_0+p^e, \qquad x_0+2p^e, \qquad \dots \qquad x_0+(p-2)p^e \qquad \text{and} \qquad x_0+(p-1)p^e.$$

So we are looking for a solution of the form

$$x_0 + tp^e,$$

where t is an integer, that is, we are trying to find t such that

$$f(x_0 + tp^e) \equiv 0 \mod p^{e+1}.$$

Note that if $n = tp^e$ then h^2, h^3, $\dots$, are all zero modulo p^{e+1}. So if we use the Taylor series expansion, we don't just get an approximation, we get an identity,

$$f(x_0 + tp^e) \equiv f(x_0) + f'(x_0)tp^e \mod p^{e+1}.$$

If we want the LHS to be zero, this says

$$tp^e f'(x_0) \equiv -f(x_0) \mod p^{e+1}.$$

By assumption there is an integer c such that $f(x_0) = cp^e$. So, cancelling the common factor of p^e, we get the linear congruence

$$tf'(x_0) \equiv c \mod p.$$

There are three cases.

(1) $f'(x_0)$ is divisible by p and c is not. There are no solutions in this case.
(2) Both $f'(x_0)$ and c are divisible by p. There are p solutions in this case.
(3) $f'(x_0)$ is not divisible by p. There is one solution in this case.

We think of the first and second case as being degenerate. Both cases are characterised by the fact that $f'(x_0) = 0$, modulo p. We call x_0 a **singular solution**. In case (3) we can solve for t, using the usual formula.

To summarise, if we start with a solution x_0 to the equation

$$f(x) \equiv 0 \mod p,$$

and $f'(x_0) \neq 0 \mod p$ then we can successive solutions, modulo higher and higher powers of p. If x_0 is a singular solution then, at each step, either there are no solutions modulo a higher power of p, or there are p solutions.

In fact the hardest part of this process is to find the solutions modulo p, but that is another story.