Hensel's lemma

From Wikipedia, the free encyclopedia

In mathematics, **Hensel's lemma**, also known as **Hensel's lifting lemma**, named after Kurt Hensel, is a result in modular arithmetic, stating that if a polynomial equation has a simple root modulo a prime number p, then this root corresponds to a unique root of the same equation modulo any higher power of p, which can be found by iteratively "lifting" the solution modulo successive powers of p. More generally it is used as a generic name for analogues for complete commutative rings (including p-adic fields in particular) of the Newton method for solving equations. Since p-adic analysis is in some ways simpler than real analysis, there are relatively neat criteria guaranteeing a root of a polynomial.

Contents

Statement

Let $f(x)$ be a polynomial with integer (or p-adic integer) coefficients, and let m,k be positive integers such that $m \le k$. If r is an integer such that

$$f(r) \equiv 0 \pmod{p^k} \text{ and } f'(r) \not\equiv 0 \pmod{p}$$

then there exists an integer s such that

$$f(s) \equiv 0 \pmod{p^{k+m}} \text{ and } r \equiv s \pmod{p^k}.$$

Furthermore, this s is unique modulo $p^{k+\mathrm{m}}$, and can be computed explicitly as

$$s = r + tp^k \text{ where } t = -\frac{f(r)}{p^k} \cdot (f'(r)^{-1}).$$

In this formula for t, the division by p^k denotes ordinary integer division (where the remainder will be 0), while negation, multiplication, and multiplicative inversion $f'(r)^{-1}$ are performed in $\mathbb{Z}/p^m\mathbb{Z}$.

As an aside, if $f'(r) \equiv 0 \pmod{p}$, then 0, 1, or several s may exist (see Hensel Lifting below).

Derivation

The lemma derives from considering the Taylor expansion of *f* around *r*. From $r \equiv s \pmod{p^k}$, we see that *s* has to be of the form $s = r + tp^k$ for some integer *t*. Expanding $f(r + tp^k)$ gives

$$f(r + tp^k) = f(r) + tp^k \cdot f'(r) + O(p^{2k}).$$

Reducing both sides modulo p^{k+m}, we see that for $f(s) \equiv 0 \pmod{p^{k+m}}$ to hold, we need

$$0 \equiv f(r + tp^k) \equiv f(r) + tp^k \cdot f'(r) \pmod{p^{k+m}}$$

where the $O(p^{2k})$ terms vanish because $k+m \le 2k$. Then we note that $f(r) = zp^k$ for some integer *z* since *r* is a root of *f* mod p^k, so

$$0 \equiv (z + tf'(r))p^k \pmod{p^{k+m}},$$

which is to say

$$0 \equiv z + tf'(r) \pmod{p^m}.$$

Then substituting back $f(r)/p^k$ for *z* and solving for *t* in $\mathbb{Z}/p^m\mathbb{Z}$ gives the explicit formula for *t* mentioned above. The assumption that $f'(r)$ is not divisible by *p* ensures that $f'(r)$ has an inverse mod p^m which is necessarily unique. Hence a solution for *t* exists uniquely modulo p^m, and *s* exists uniquely modulo p^{k+m}.

Hensel Lifting

Using the lemma, one can "lift" a root *r* of the polynomial *f* mod p^k to a new root *s* mod p^{k+1} such that $r \equiv s$ mod p^k (by taking m=1; taking larger *m* also works). In fact, a root mod p^{k+1} is also a root mod p^k, so the roots mod p^{k+1} are precisely the liftings of roots mod p^k. The new root *s* is congruent to *r* mod *p*, so the new root also satisfies $f'(s) \equiv f'(r) \not\equiv 0 \pmod{p}$. So the lifting can be repeated, and starting from a solution r_k of $f(x) \equiv 0 \pmod{p^k}$ we can derive a sequence of solutions r_{k+1}, r_{k+2}, ... of the same congruence for successively higher powers of *p*, provided $f'(r_k) \not\equiv 0 \pmod{p}$ for the initial root r_k. This also shows that *f* has the same number of roots mod p^k as mod p^{k+1}, mod p^{k+2}, or any other higher power of *p*, provided the roots of *f* mod p^k are all simple.

What happens to this process if *r* is not a simple root mod *p*? If we have a root mod p^k at which the derivative mod *p* is 0, then there is *not* a unique lifting of a root mod p^k to a root mod p^{k+1}: either there is no lifting to a root mod p^{k+1} or there are multiple choices:

if $f(r) \equiv 0 \bmod p^k$ and $f'(r) \equiv 0 \bmod p$, then
$s \equiv r \bmod p^k \Rightarrow f(s) \equiv f(r) \bmod p^{k+1}$.

That is, $f(r + tp^k) \equiv 0 \bmod p^{k+1}$ for all integers *t*. Therefore if $f(r) \not\equiv 0 \bmod p^{k+1}$, then there is no lifting of *r* to a root of *f*(*x*) mod p^{k+1}, while if $f(r) \equiv 0 \bmod p^{k+1}$, then every lifting of *r* to modulus p^{k+1} is a root of *f*(*x*) mod p^{k+1}.

To see the difficulty that can arise in a concrete example, take $p = 2$, $f(x) = x^2 + 1$, and $r = 1$. Then $f(1) \equiv 0$ mod 2 and $f'(1) \equiv 0$ mod 2. We have $f(1) = 2 \not\equiv 0$ mod 4 and no lifting of 1 to modulus 4 is a root of $f(x)$ mod 4. On the other hand, if we take $f(x) = x^2 - 17$ and then 1 is a root of $f(x)$ mod 2 and for every positive integer k there is more than one lifting of 1 mod 2 to a root of $f(x)$ mod 2^k.

Hensel's Lemma for *p*-adic Numbers

In the p-adic numbers, where we can make sense of rational numbers modulo powers of p as long as the denominator is not a multiple of p, the recursion from r_k (roots mod p^k) to r_{k+1} (roots mod p^{k+1}) can be expressed in a much more intuitive way. Instead of choosing t to be an(y) integer which solves the congruence $tf'(r_k) \equiv -(f(r_k)/p^k) \bmod p^m$, let t be the rational number $-(f(r_k)/p^k)/f'(r_k)$ (the p^k here is not really a denominator since $f(r_k)$ is divisible by p^k). Then set

$$r_{k+1} = r_k + tp^k = r_k - \frac{f(r_k)}{f'(r_k)}.$$

This fraction may not be an integer, but it is a p-adic integer, and the sequence of numbers r_k converges in the p-adic integers to a root of $f(x) = 0$. Moreover, the displayed recursive formula for the (new) number r_{k+1} in terms of r_k is precisely Newton's method for finding roots to equations in the real numbers.

By working directly in the p-adics and using the p-adic absolute value, there is a version of Hensel's lemma which can be applied even if we start with a solution of $f(a) \equiv 0$ mod p such that $f'(a) \equiv 0$ mod p. We just need to make sure the number $f'(a)$ is not exactly 0. This more general version is as follows: if there is an integer a which satisfies $|f(a)|_p < |f'(a)|_p^2$, then there is a unique p-adic integer b such $f(b) = 0$ and $|b-a|_p < |f'(a)|_p$. The construction of b amounts to showing that the recursion from Newton's method with initial value a converges in the p-adics and we let b be the limit. The uniqueness of b as a root fitting the condition $|b-a|_p < |f'(a)|_p$ needs additional work.

The statement of Hensel's lemma given above (taking $m = 1$) is a special case of this more general version, since the conditions that $f(a) \equiv 0$ mod p and $f'(a) \not\equiv 0$ mod p say that $|f(a)|_p < 1$ and $|f'(a)|_p = 1$.

Examples

Suppose that p is an odd prime number and a is a quadratic residue modulo p that is nonzero mod p. Then Hensel's lemma implies that a has a square root in the ring of p-adic integers $\mathbf{Z}_p$. Indeed, let $f(x)=x^2-a$. Its derivative is $2x$, so if r is a square root of a mod p we have

$$f(r) = r^2 - a \equiv 0 \bmod p \text{ and } f'(r) = 2r \not\equiv 0 \bmod p,$$

where the second condition depends on p not being 2. The basic version of Hensel's lemma tells us that starting from $r_1 = r$ we can recursively construct a sequence of integers $\{ r_k \}$ such that

$$r_{k+1} \equiv r_k \bmod p^k, \quad r_k^2 \equiv a \bmod p^k.$$

This sequence converges to some p-adic integer b and $b^2=a$. In fact, b is the unique square root of a in $\mathbf{Z}_p$ congruent to r_1 modulo p. Conversely, if a is a perfect square in $\mathbf{Z}_p$ and it is not divisible by p then it is a nonzero quadratic residue mod p. Note that the quadratic reciprocity law allows one to easily test whether a is a nonzero quadratic residue mod p, thus we get a practical way to determine which p-adic numbers (for p odd) have a p-adic square root, and it can be extended to cover the case p=2 using the more general version of Hensel's lemma (an example with 2-adic square roots of 17 is given later).

To make the discussion above more explicit, let us find a "square root of 2" (the solution to $x^2 - 2 = 0$) in the 7-adic integers. Modulo 7 one solution is 3 (we could also take 4), so we set $r_1 = 3$. Hensel's lemma then allows us to find r_2 as follows:

$$f(r_1) = 3^2 - 2 = 7$$
$$f(r_1)/p^1 = 7/7 = 1$$
$$f'(r_1) = 2r_1 = 6$$
$$tf'(r_1) \equiv -(f(r_1)/p^{k-1}) \bmod p, \text{ that is, } t \cdot 6 \equiv -1 \bmod 7$$
$$\Rightarrow t = 1$$
$$r_2 = r_1 + tp^1 = 3 + 1 \cdot 7 = 10 = 13_7.$$

And sure enough, $10^2 \equiv 2 \bmod 7^2$. (If we had used the Newton method recursion directly in the 7-adics, then $r_2 = r_1 - f(r_1)/f'(r_1) = 3 - 7/6 = 11/6$, and $11/6 \equiv 10 \bmod 7^2$.)

We can continue and find $r_3 = 108 = 3 + 7 + 2 \cdot 7^2 = 213_7$. Each time we carry out the calculation (that is, for each successive value of k), one more base 7 digit is added for the next higher power of 7. In the 7-adic integers this sequence converges, and the limit is a square root of 2 in $\mathbf{Z}_7$ which has initial 7-adic expansion

$$3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 7^4 + 2 \cdot 7^5 + 7^6 + 2 \cdot 7^7 + 4 \cdot 7^8 + \cdots.$$

If we started with the initial choice $r_1 = 4$ then Hensel's lemma would produce a square root of 2 in $\mathbf{Z}_7$ which is congruent to 4 (mod 7) instead of 3 (mod 7) and in fact this second square root would be the negative of the first square root (which is consistent with 4 = -3 mod 7).

As an example where the original version of Hensel's lemma is not valid but the more general one is, let $f(x) = x^2 - 17$ and $a = 1$. Then $f(a) = -16$ and $f'(a) = 2$, so $|f(a)|_2 < |f'(a)|_2^2$, which implies there is a unique 2-adic integer b satisfying $b^2 = 17$ and $|b - a|_2 < |f'(a)|_2 = 1/2$, i.e., $b \equiv 1 \bmod 4$. There are two square roots of 17 in the 2-adic integers, differing by a sign, and although they are congruent mod 2 they are not congruent mod 4. This is consistent with the general version of Hensel's lemma only giving us a unique 2-adic square root of 17 that is congruent to 1 mod 4 rather than mod 2. If we had started with the initial approximate root $a = 3$ then we could apply the more general Hensel's lemma again to find a unique 2-adic square root of 17 which is congruent to 3 mod 4. This is the other 2-adic square root of 17.

In terms of lifting roots of $x^2 - 17$ from one modulus 2^k to the next 2^{k+1}, the lifts starting with the root 1 mod 2 are as follows:

1 mod 2 --> 1, 3 mod 4
1 mod 4 --> 1, 5 mod 8 and 3 mod 4 ---> 3, 7 mod 8
1 mod 8 --> 1, 9 mod 16 and 7 mod 8 ---> 7, 15 mod 16, while 3 mod 8 and 5 mod 8 don't lift to roots mod 16
9 mod 16 --> 9, 25 mod 32 and 7 mod 16 --> 7, 23 mod 16, while 1 mod 16 and 15 mod 16

don't lift to roots mod 32.

For every k at least 3, there are *four* roots of x^2 - 17 mod 2^k, but if we look at their 2-adic expansions we can see that in pairs they are converging to just *two* 2-adic limits. For instance, the four roots mod 32 break up into two pairs of roots which each look the same mod 16:

$9 = 1 + 2^3$ and $25 = 1 + 2^3 + 2^4$, $7 = 1 + 2 + 2^2$ and $23 = 1 + 2 + 2^2 + 2^4$.

The 2-adic square roots of 17 have expansions

$1 + 2^3 + 2^5 + 2^6 + 2^7 + 2^9 + 2^{10} + \ldots, 1 + 2 + 2^2 + 2^4 + 2^8 + 2^{11} \ldots$

Another example where we can use the more general version of Hensel's lemma but not the basic version is a proof that any 3-adic integer $c \equiv 1$ mod 9 is a cube in $\mathbf{Z}_3$. Let $f(x) = x^3$ - c and take initial approximation $a = 1$. The basic Hensel's lemma can't be used to find roots of $f(x)$ since $f'(r) \equiv 0$ mod 3 for every r. To apply the general version of Hensel's lemma we want $|f(1)|_3 < |f'(1)|_3{}^2$, which means $c \equiv 1$ mod 27. That is, if $c \equiv 1$ mod 27 then the general Hensel's lemma tells us $f(x)$ has a 3-adic root, so c is a 3-adic cube. However, we wanted to have this result under the weaker condition that $c \equiv 1$ mod 9. If $c \equiv 1$ mod 9 then $c \equiv 1$, 10, or 19 mod 27. We can apply the general Hensel's lemma three times depending on the value of c mod 27: if $c \equiv 1$ mod 27 then use $a = 1$, if $c \equiv 10$ mod 27 then use $a = 4$ (since 4 is a root of $f(x)$ mod 27), and if $c \equiv 19$ mod 27 then use $a = 7$. (It is not true that every $c \equiv 1$ mod 3 is a 3-adic cube, e.g., 4 is not a 3-adic cube since it is not a cube mod 9.)

In a similar way, after some preliminary work Hensel's lemma can be used to show that for any *odd* prime number p, any p-adic integer c which is 1 mod p^2 is a p-th power in $\mathbf{Z}_p$. (This is false when p is 2.)

Generalizations

Suppose A is a commutative ring, complete with respect to an ideal $\mathfrak{m}_A$, and let $f(x) \in A[x]$ be a polynomial with coefficients in A. Then if $a \in A$ is an "approximate root" of f in the sense that it satisfies

$$f(a) \equiv 0 \bmod f'(a)^2\mathfrak{m}$$

then there is an exact root $b \in A$ of f "close to" a; that is,

$$f(b) = 0$$

and

$$b \equiv a \bmod f'(a)\mathfrak{m}.$$

Further, if $f'(a)$ is not a zero-divisor then b is unique.

As a special case, if $f(a) \equiv 0 \bmod \mathfrak{m}$ and $f'(a)$ is a unit in A then there is a unique solution to $f(b) = 0$ in A such that $b \equiv a \bmod \mathfrak{m}$.

This result can be generalized to several variables as follows:

Theorem: Let A be a commutative ring that is complete with respect to an ideal $\mathbf{m} \subset A$ and $f_i(\mathbf{x}) \in A[x_1, \ldots, x_n]$ for $i = 1,\ldots,n$ be a system of n polynomials in n variables over A. Let $\mathbf{f} = (f_1,\ldots,f_n)$, viewed as a mapping from A^n to A^n, and let $J_{\mathbf{f}}(\mathbf{x})$ be the Jacobian matrix of $\mathbf{f}$. Suppose some $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$ is an approximate solution to $\mathbf{f} = \mathbf{0}$ in the sense that

$$f_i(\mathbf{a}) \equiv 0 \bmod (\det \mathrm{J}_{\mathbf{f}}(\mathbf{a}))^2\mathbf{m}$$

for $1 \le i \le n$. Then there is some $\mathbf{b} = (b_1, \ldots, b_n)$ in A^n satisfying $\mathbf{f}(\mathbf{b}) = \mathbf{0}$, i.e.,

$$f_i(\mathbf{b}) = 0 \text{ for all } i,$$

and furthermore this solution is "close" to $\mathbf{a}$ in the sense that

$$b_i \equiv a_i \bmod J_{\mathbf{f}}(\mathbf{a})\mathbf{m}$$

for $1 \le i \le n$.

As a special case, if $f_i(\mathbf{a}) \equiv 0 \bmod \mathbf{m}$ for all i and $\det \mathrm{J}_{\mathbf{f}}(\mathbf{a})$ is a unit in A then there is a solution to $\mathbf{f}(\mathbf{b}) = \mathbf{0}$ with $b_i \equiv a_i \bmod \mathbf{m}$ for all i.

When $n = 1$, $\mathbf{a} = a$ is an element of A and $J_{\mathbf{f}}(\mathbf{a}) = J_f(a)$ is $f'(a)$. The hypotheses of this multivariable Hensel's lemma reduce to the ones which were stated in the one-variable Hensel's lemma.

Related concepts

Completeness of a ring is not a necessary condition for the ring to have the Henselian property: Goro Azumaya in 1950 defined a commutative local ring satisfying the Henselian property for the maximal ideal $\mathbf{m}$ to be a **Henselian ring**.

Masayoshi Nagata proved in the 1950s that for any commutative local ring A with maximal ideal $\mathbf{m}$ there always exists a smallest ring A^{h} containing A such that A^{h} is Henselian with respect to $\mathbf{m}A^{\mathrm{h}}$. This A^{h} is called the **Henselization** of A. If A is noetherian, A^{h} will also be noetherian, and A^{h} is manifestly algebraic as it is constructed as a limit of étale neighbourhoods. This means that A^{h} is usually much smaller than the completion $\hat{A}$ while still retaining the Henselian property and remaining in the same category.

See also

- Hasse–Minkowski theorem
- Newton polygon

References

- Eisenbud, David (1995), *Commutative algebra*, Graduate Texts in Mathematics **150**, Berlin, New York: Springer-Verlag, ISBN 978-0-387-94269-8, MR 1322960 (http://www.ams.org/mathscinet-getitem?mr=1322960)
- Milne, J. G. (1980), *Étale cohomology*, Princeton University Press, ISBN 978-0-691-08238-7

Categories: Modular arithmetic | Commutative algebra | Lemmas

---

- This page was last modified on 18 March 2014 at 11:55.