

Hensel's Lemma

Jonathan L.F. King

University of Florida, Gainesville FL 32611-2082, USA

squash@ufl.edu

Webpage <http://squash.1gainesville.com/>

27 March, 2023 (at 10:25)

Notation. Quantities $x, y, M, m, K, k \dots$ are integers, by default. Recall " $x \equiv_m y$ " means $[x - y] \mid m$. Thus \equiv_0 is equality, $=$, in the integers.

1: Tools. Consider $n \in \mathbb{Z}$, $K \in \mathbb{N}$, $M \in \mathbb{Z}_+$ and an intpoly $h()$. Then:

1a: Ratio $\llbracket n \downarrow K \rrbracket / K!$ is an integer.

1b: Differentiating, $h^{(K)}/K!$ is an intpoly.

1c: $\forall x, y: [x \equiv_M y] \Rightarrow [h(x) \equiv_M h(y)]$.

1d: If $N := \text{Deg}(h) \geq 1$, then for complex numbers Z, b :

$$h(Z + b) = h(Z) + [h'(Z) \cdot b] + \sum_{K=2}^N \frac{h^{(K)}(Z)}{K!} \cdot b^K. \diamond$$

Pf of (1a). For $n \geq K \geq 0$, set $j := n - K$ and note $\llbracket n \downarrow K \rrbracket / K!$ equals $j! \cdot \binom{n}{K, j}$, which is an integer. Hence degree- K polynomial $f(x) := \llbracket x \downarrow K \rrbracket / K!$ is integer-valued at $K+1$ consecutive integers [indeed, for all integers $x \in [K.. \infty)$], and thus (exercise) is integer-valued at all integers. [However, the coefficients of f need not be integers.] \diamond

Pf of (1b). Write $h(x)$ as $\sum_{j=0}^{\text{Finite}} C_j x^j$. For $n \geq K$, the coefficient of x^{n-K} in $\frac{h^{(K)}(x)}{K!}$ is $C_n \cdot \frac{\llbracket n \downarrow K \rrbracket}{K!}$. \diamond

Pf of (1d). Since h is a degree- N polynomial, its N^{th} -Taylor-poly is h itself. \diamond

Hensel's Setting. Fix an intpoly $f()$ of degree $N \geq 1$, and fix a prime P .

Use \equiv^{ℓ} as a synonym for \equiv_{P^ℓ} .

E.g. $257 \equiv^3 7$ means $[257 - 7] \mid P^3$. For a *level* $\ell \in \mathbb{Z}_+$, an integer α is an " ℓ^{th} -root (of f)" if

$$f(\alpha) \equiv^{\ell} 0.$$

For $\ell = 2, 3, \dots$, we seek ℓ^{th} -roots of f , starting from a given $\ell=1$ root Z , i.e $f(Z) \equiv_P 0$.

Set $Z_1 := Z$. We proceed by induction on ℓ .

2: Hensel's, non-singular. Suppose $f(Z) \equiv_P 0$ and $f'(Z) \not\equiv_P 0$. Let $U := \langle 1/f'(Z) \rangle_P$. Setting $Z_1 := Z$, for $\ell = 1, 2, \dots$ define

$$2a: Z_{\ell+1} := Z_\ell - [f(Z_\ell) \cdot U], \pmod{P^{\ell+1}}.$$

This satisfies that

$$2b: Z_{\ell+1} \equiv^{\ell} Z_\ell \quad \text{and}$$

$$2c: f(Z_{\ell+1}) \equiv^{\ell+1} 0. \quad \diamond$$

Proof. Fix an $\ell \in \mathbb{Z}_+$ st. $f(Z_\ell) \equiv^{\ell} 0$ and $Z_\ell \equiv_P Z$. We solve for those values $t \in \mathbb{Z}_P$, if any, such that sum

$$*: Z_{\ell+1} := Z_\ell + tP^\ell$$

satisfies (2c). Let $\alpha := Z_\ell$. We apply Taylor's thm to $f(\alpha + tP^\ell)$. Its k^{th} -term is

$$\dagger: \frac{f^{(k)}(\alpha)}{k!} \cdot t^k P^{k\ell}.$$

When $k \geq 2$, then $k\ell \geq 2\ell \geq \ell+1$, since $\ell \geq 1$. Hence $P^{k\ell} \equiv^{\ell+1} 0$. Ratio $[f^{(k)}(\alpha)/k!]$ is an integer, courtesy (1b). Hence (\dagger) is $\equiv^{\ell+1} 0$. Consequently,

$$f(\alpha + tP^\ell) \equiv^{\ell+1} \underbrace{f(\alpha)}_{(\dagger) \text{ at } k=0.} + \underbrace{[f'(\alpha) \cdot tP^\ell]}_{(\dagger) \text{ at } k=1.}.$$

We seek a t making this zero, mod $P^{\ell+1}$; i.e, that

$$\ddagger: t \cdot f'(\alpha) \cdot P^\ell \equiv^{\ell+1} -f(\alpha).$$

By hypothesis, $f(\alpha) \not\equiv P^\ell$. So (\ddagger) is equivalent to

$$2d: t \cdot f'(\alpha) \equiv_P -\frac{f(\alpha)}{P^\ell}. \quad [\text{Division is in } \mathbb{Z}].$$

By our hypothesis, $\alpha \equiv_P Z$ and so U is the mod- P reciprocal of $f'(\alpha)$. Thus

$$t \equiv_P -\left[\frac{f(\alpha)}{P^\ell}\right] \cdot U. \quad [\text{Division is in } \mathbb{Z}].$$

Plugging this into $(*)$ gives (2a). \diamond

NB: Please ignore the singular case, which is below.

Defn. Fix a posint T . For a level ℓ satisfying

$$3a: \quad \ell \geq 1 + 2T,$$

say that an integer α is “ ℓ, T -good” if

$$3b: \quad f(\alpha) \stackrel{\ell}{\equiv} 0, \quad \text{and the derivative satisfies}$$

$$3c: \quad f'(\alpha) \parallel P^T. \quad \square$$

4.0: Hensel singular-thm. Fix a posint T , and let “ ℓ -good” mean ℓ, T -good.

Consider a level ℓ and an ℓ -good integer α . There there exists a unique $m \in [0..P)$ such that

$$\beta := \alpha + mP^{\ell-T}$$

is $[\ell+1]$ -good. \diamond

Proof. Inequality (3a) gives $\ell - T \geq T+1$. Thus each $\beta \equiv_{P^{\ell+1}} \alpha$. Applying (1) to intpoly $f'()$ gives

$$f'(\beta) \equiv_{P^{\ell+1}} f'(\alpha).$$

Thus (3c) forces $f'(\beta) \parallel P^T$, regardless of m .

Of course, $\ell+1 \geq \ell \geq 1 + 2T$, so to produce β which is $[\ell+1]$ -good, we must exhibit an m with $f(\beta) \parallel P^{\ell+1}$.

Making an $[\ell+1]$ -root β . For an exponent $e \in \mathbb{N}$ and all $m, x \in \mathbb{Z}$, we can expand the e^{th} -power as

$$\begin{aligned} [x + mP^{\ell-T}]^e &= x^e + mP^{\ell-T} \cdot \binom{e}{1} x^{e-1} \\ &\quad + m^2 P^{2[\ell-T]} \cdot \binom{e}{2} x^{e-2} + \dots. \end{aligned}$$

Since (3a) implies $2[\ell - T] \geq \ell + 1$, we have that

$$\begin{aligned} [x + mP^{\ell-T}]^e &\stackrel{\ell+1}{\equiv} x^e + mP^{\ell-T} \cdot \binom{e}{1} x^{e-1} \\ &= x^e + mP^{\ell-T} \cdot \frac{d}{dx}(x^e). \end{aligned}$$

Write $f(x)$ as $\sum_{e=0}^N C_e x^e$. Multiplying the above by C_e , then summing, gives

$$4.1: \quad f(x + mP^{\ell-T}) \stackrel{\ell+1}{\equiv} f(x) + mP^{\ell-T} \cdot f'(x),$$

where $\beta_m := \alpha + mP^{\ell-T}$.

Dividing. Courtesy (3c), we can write

$$f'(\alpha) = D \cdot P^T, \quad \text{with } D \perp P.$$

And (3b) gives $f(\alpha) = E \cdot P^\ell$ with $E \in \mathbb{Z}$. So we can rewrite (4.1) as

$$4.2: \quad f(\beta_m) \stackrel{\ell+1}{\equiv} [E + mD] \cdot P^\ell.$$

Since $D \perp P$, there is a unique $m \in [0..P)$ making $E + mD \equiv_P 0$. That is the unique value making $f(\beta_m) \equiv_{P^{\ell+1}} 0$. \diamond

Filename: Problems/NumberTheory/hensel-lemma.latex
As of: Thursday 18Apr2013. Typeset: 27Mar2023 at 10:25.