Hensel's Lemma

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
31 January, 2017 (at *08:46*)

Notation. Quantities $x, y, M, m, K, k \ldots$ are integers, by default. Recall "$x \equiv_m y$" means $[x-y] \bullet m$. 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 $[\![n!K]\!]/K!$ is an integer.*

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

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

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

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

Pf of (1a). For $n \geqslant K \geqslant 0$, set $j := n-K$ and note $[\![n!K]\!]/K!$ equals $j! \cdot \binom{n}{K,j}$, which is an integer. Hence degree-K polynomial $f(x) := [\![x!K]\!]/K!$ 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 *coeffs* of f need not be integers.] ♦

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

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

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

Use $\stackrel{\ell}{\equiv}$ as a synonym for $\equiv_{P^\ell}$, e.g, $257 \stackrel{3}{\equiv} 7$ means $[257-7] \bullet P^3$. For a ***level*** $\ell \in \mathbb{Z}_+$, an integer $\boldsymbol{\alpha}$ is an **"ℓ-*root*** (of f)**"** if

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

For $\ell = 2, 3, \ldots$, we seek ℓ^{th}-roots of f, starting from a given ℓ=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 $f(Z) \equiv_P 0$ yet $f'(Z) \not\equiv_P 0$. Let $U := \langle 1/f'(Z) \rangle_P$. Setting $Z_1 := Z$, for $\ell = 1, 2, \ldots$ define*

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

This satisfies that

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

2c: $$f(Z_{\ell+1}) \stackrel{\ell+1}{\equiv} 0. \qquad \diamondsuit$$

Proof. Fix an $\ell \in \mathbb{Z}_+$ st. $f(Z_\ell) \stackrel{\ell}{\equiv} 0$ 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 $\boldsymbol{\alpha} := Z_\ell$. We apply Taylor's thm to $f(\boldsymbol{\alpha} + tP^\ell)$. Its k^{th} term is

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

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

$$f(\boldsymbol{\alpha} + tP^\ell) \stackrel{\ell+1}{\equiv} f(\boldsymbol{\alpha}) + [f'(\boldsymbol{\alpha})\cdot tP^\ell].$$

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

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

By hypothesis, $f(\boldsymbol{\alpha}) \bullet P^\ell$. So (†) is equivalent to

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

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

$$t \equiv_P -\Big[\frac{f(\boldsymbol{\alpha})}{P^\ell}\Big]\cdot U. \quad [\textit{Division is } \underline{\textit{in } \mathbb{Z}}.]$$

Plugging this into $(*)$ gives (2a). ♦

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

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

3a: $$\ell \geqslant 1+2T,$$

say that an integer $\boldsymbol{\alpha}$ is "***ℓ,T-good***" if

3b: $f(\boldsymbol{\alpha}) \overset{\ell}{\equiv} 0$, and the derivative satisfies

3c: $f'(\boldsymbol{\alpha}) \parallel\!\bullet\, \mathsf{P}^T$. □

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 $\boldsymbol{\alpha}$. There there exists a unique $m \in [0 \,..\, \mathsf{P})$ such that

$$\boldsymbol{\beta} := \boldsymbol{\alpha} + m\mathsf{P}^{\ell-T}$$

is $[\ell+1]$-good. ◊

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

$$f'(\boldsymbol{\beta}) \equiv_{\mathsf{P}^{T+1}} f'(\boldsymbol{\alpha}).$$

Thus (3c) forces $f'(\boldsymbol{\beta}) \parallel\!\bullet\, \mathsf{P}^T$, regardless of m.

Of course, $\ell+1 \geqslant \ell \geqslant 1+2T$, so to produce $\boldsymbol{\beta}$ which is $[\ell+1]$-good, we must exhibit an m with $f(\boldsymbol{\beta}) \,|\!\bullet\, \mathsf{P}^{\ell+1}$.

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

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

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

$$\begin{aligned}[x + m\mathsf{P}^{\ell-T}]^e &\overset{\ell+1}{\equiv} x^e + m\mathsf{P}^{\ell-T} \cdot \binom{e}{1} x^{e-1} \\ &= x^e + m\mathsf{P}^{\ell-T} \cdot \tfrac{\mathrm{d}}{\mathrm{d}x}(x^e).\end{aligned}$$

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

4.1: $$f(x + m\mathsf{P}^{\ell-T}) \overset{\ell+1}{\equiv} f(x) + m\mathsf{P}^{\ell-T} \cdot f'(x),$$

where $\boldsymbol{\beta}_m := \boldsymbol{\alpha} + m\mathsf{P}^{\ell-T}$.

Dividing. Courtesy (3c), we can write

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

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

4.2: $$f(\boldsymbol{\beta}_m) \overset{\ell+1}{\equiv} [E + mD] \cdot \mathsf{P}^\ell.$$

Since $D \perp \mathsf{P}$, there is a *unique* $m \in [0 \,..\, \mathsf{P})$ making $E + mD \equiv_{\mathsf{P}} 0$. That is the unique value making $f(\boldsymbol{\beta}_m) \equiv_{\mathsf{P}^{\ell+1}} 0$. ♦

Filename: `Problems/NumberTheory/hensel-lemma.latex`
As of: *Thursday 18Apr2013.* Typeset: *31Jan2017 at 08:46.*