Hensel's Lemma

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Suppose V to be an affine variety defined over $\mathbb{Q}_p$ with coefficients in $\mathbb{Z}_p$, say embedded in $\mathbb{Z}_p^d$. This means that it is the zero set of a set of polynomials with coefficients in $\mathbb{Z}_p$. Hence for each m one can consider its zero set in $(\mathbb{Z}/p^m)^d$, those points satisfying these equations modulo p^m. *What can one say about the number of points defined over $\mathbb{Z}/p^m$, as m grows large?* Every point modulo p^{m+1} determines a point modulo p^m. *What is the image of this reduction map? Under what circumstances is this map surjective? What points in the zero set in $(\mathbb{Z}/p^m)^d$ are in the image of the zero set in $\mathbb{Z}_p^d$?* Hensel's Lemma answers these questions. The well known case is valid for V a smooth scheme over $\mathbb{Z}_p$. But there is also a version when V is non-singular as a variety over $\mathbb{Q}_p$. In the present version of this note, I'll look only at the case V is a non-singular hypersurface $f(x) = 0$.

After §1, the situation will be a little more general:

$$
\begin{aligned}
\mathfrak{k} &= \text{a local field} \\
\mathfrak{o} &= \text{the integers of } \mathfrak{k} \\
\mathfrak{p} &= \text{the maximal ideal of } \mathfrak{o} \\
\varpi &= \text{a generator of } \mathfrak{p}, \text{ so } \mathfrak{p} = (\varpi) \\
\mathbb{F}_q &= \mathfrak{o}/\mathfrak{p}\,.
\end{aligned}
$$

Thus $q = p^r$ for some prime number p. Let $\equiv_n$ mean congruence modulo $\mathfrak{p}^n$.

Contents

1. Introduction [Hensel.tex]

Let's look at a simple example, a variety of dimension 0, with $f(x) = x^2 - a$ and a in $\mathbb{Z}_p$.

Suppose at first p to be odd. If the image of a modulo p is not a square in $\mathbb{Z}/p$ there cannot be any solutions in $\mathbb{Z}_p$. Two cases remain: the image of a in $\mathbb{Z}/p$ is (a) a non-zero square or (b) 0. The second case is singular, and I'll postpone looking at it.

So now assume that a is a unit square modulo p. There are two solutions in $\mathbb{Z}/p$. What about modulo p^n? We proceed by induction on n. Suppose that x_n is a solution modulo p^n and that we want to find all those x modulo p^{n+1} which are congruent to x_n modulo p^n. We may express

$$x = x_n + hp^n$$

with $x_n^2 \equiv_n a$. Can we find h such that $x^2 \equiv_{n+1} a$? We must solve

$$(x_n + hp^n)^2 = x_n^2 + 2hx_np^n + h^2p^{2n} \equiv_{n+1} a\,.$$

Since $n \geq 1$, the last term lies in p^{n+1}, so we may ignore it, and it remains to solve

$$x_n^2 + 2hp^nx_n \equiv_{n+1} a\,.$$

But then we may set

$$h = -\frac{x_n^2 - a}{2x_n p^n},$$

which is legitimate because $2x_n$ is invertible in $\mathfrak{o}$ and ϖ^n divides $x_n^2 - a$. One important point here is that h is unique modulo p, hence hp^n unique modulo p^{n+1}. At any rate, the process continues, producing a sequence that converges to some value of $\sqrt{a}$. In effect we are applying the p-adic analogue of Newton's method—we start with a good approximation of a square root and find a sequence of better approximations. The conclusion is that *if p is odd and a modulo p is a non-zero square in $\mathbb{Z}/p$ there are exactly two square roots of a in $\mathbb{Z}_p$.*

There are other ways in which one can arrive at this conclusion, such as one using the binomial series for $(1+x)^{1/2}$, but I'll ignore them since my intention is to describe a tool, not a specific conclusion.

The case $p = 2$ is more interesting. I'll illustrate what happens by looking at a couple of specific examples. First take $a = 5$. Then a is a square modulo 2 and 4, but not modulo 8, so it cannot be a square in $\mathbb{Z}_2$. It is natural to ask, *how deep does one have to look in order to apply this sort of test?* Next, try $a = 17$. Here a is a square modulo 16. As one can check quickly, there is one solution in $\mathbb{Z}/2$, two in $\mathbb{Z}/4$, four solutions in $\mathbb{Z}/8$, and four in $\mathbb{Z}/16$. Does this number remain fixed for $n \geq 3$? Yes, but for slightly peculiar reasons. After all, there cannot be four square roots of any number in $\mathbb{Z}_2$, so something not quite straightforward has to take place.

In $\mathbb{Z}/8$, the square of every unit is equal to 1. But in $\mathbb{Z}/16$, the solutions of $x^2 = 1$ are ± 1, ± 7—i.e. only half the units. Their images in $\mathbb{Z}/8$ give only ± 1, which is to say that only half of the solutions in $\mathbb{Z}/8$ lift to solutions in $\mathbb{Z}/16$. And so it continues—there are indeed 4 solutions in each $\mathbb{Z}/2^n$ with $n \geq 3$, but only half of them at each stage lift to $\mathbb{Z}/2^{n+1}$. The reason things go wrong is more or less easy to understand—in Newton's formula the denominator factor $2x_n$ is no longer a unit, so there has to be some modification in order to make it work. Exactly how will be seen later on. The conclusion one arrives at here is that *if $a \equiv_8 1$ then there exist two square roots of a in $\mathbb{Z}_2$.* (Here, too, one might use the binomial series for $(1+8x)^{1/2}$, but it is not quite so simple to see why it converges.)

In the next section I'll explain Hensel's Lemma in the case that generalizes what happened for $x^2 - a$ when p was odd, and in the section after that I'll deal with the singular cases.

2. The non-singular case [Hensel.tex]

I shall look in this section and the next at the case when the variety is a hypersurface $f = 0$, generically non-singular. I recall that a point of the scheme $f = 0$, in which f has coefficients in the field F, is non-singular at a point x if its gradient $\nabla_f(x)$ does not vanish. That means that for some $N > 0$ we have

$$\nabla_f(x) \equiv_{N-1} 0, \quad \nabla_f(x) \not\equiv_N 0\,.$$

I shall assume in this section that $N = 1$, or equivalently that $f = 0$ in fact remains non-singular at x modulo p at the point concerned.

[hensel] **2.1. Lemma.** (Hensel's Lemma I) *Suppose $f(x)$ to be a polynomial in d variables with coefficients in $\mathfrak{o}$. Then for every solution x_n of $f(x_n) \equiv_n 0$ but $\nabla_f(x_n) \not\equiv_1 0$ there exist p^{d-1} solutions modulo $\mathfrak{p}^{n+1}$ that are $\equiv_n x_n$.*

Proof. The assumption means that $\nabla_f(x_n)$ is non-zero modulo $\mathfrak{p}$, hence that $\nabla_f(x)$ is a non-zero function on $\mathbb{F}_q^d$. We want to show that for every solution of $f(x_n) \equiv_n 0$ there exist exactly q^{d-1} modulo $\mathfrak{p}^{n+1}$ that are $\equiv_n x_n$. But if we choose an arbitrary x modulo $\mathfrak{p}^{n+1}$ with $x \equiv_n x_n$ then we can in fact find exactly q^{d-1} solutions of

$$f(x + \varpi^n a) = f(x) + \varpi^n \langle \nabla_f(x_n), a\rangle \equiv_{n+1} 0$$

by solving $\langle \nabla_f(x_n), a\rangle = -f(x_n)/\varpi^n$ for a. ▯

From this, one can construct a Cauchy sequence converging to a root of $f(x) = 0$:

[hensels-theorem] **2.2. Theorem.** *If x_n satisfies $f(x_n) \equiv 0$ and $\nabla_f(x) \not\equiv_1 0$, then there exists x in $\mathfrak{o}^d$ with $f(x) = 0$ and $x \equiv_n x_n$.*

3. The singular case [Hensel.tex]

We now look at a more complicated case. Suppose x in $\mathfrak{o}$, $f(x) \equiv_n 0$, $\nabla_f(x) \equiv_N 0$ but not $\equiv_{N+1} 0$. We have seen from examples above that we cannot expect to find $y \equiv_n x$ with $f(y) \equiv_{n+1} 0$. So we search more generally for y of the form $x + \varpi^{n-k}h$. (In the non-singular case, with $N = 0$, we may choose $k = 0$.) Now

$$f(x + \varpi^{n-k}h) = f(x) + \varpi^{n-k}\langle \nabla_f(x), h\rangle + O(\varpi^{2n-2k}) .$$

In order to make the earlier technique work, we must first require

$$2n - 2k \geq n + 1, \quad n \geq 2k + 1 .$$

Set $f(x) = c\varpi^n$, $\nabla_f(x) = d\varpi^N$ with d a non-zero vector modulo $\mathfrak{p}$. We now want to be able to solve

$$\begin{aligned} \varpi^{n-k}\langle \nabla_f(x), h\rangle &\equiv_{n+1} -c\varpi^n \\ \varpi^{n-k+N}\langle d, h\rangle &\equiv_{n+1} -c\varpi^n \\ \varpi^{N-k}\langle d, h\rangle &\equiv_1 -c \end{aligned}$$

This will be possible precisely when $k = N$, and the value of h will be unique modulo $\mathfrak{p}$.

[hensels-lemma-2] **3.1. Lemma.** (Hensels' Lemma II) *Suppose $f(x_n) \equiv_n 0$, $\nabla_f(x_n) \equiv_N 0$ but not $\equiv_{N+1} 0$. If $n \geq 2N + 1$ there exists h unique modulo $\mathfrak{p}$ such that if*

$$x_{n+1} = x_n + \varpi^{n-N}h$$

then

$$f(x_{n+1}) \equiv_{n+1} 0 .$$

Thus for $n \geq 2N + 1$ the number of solutions modulo $\mathfrak{p}^n$ remains constant, but only $1/q^N$ of the solutions modulo $\mathfrak{p}^n$ lift to solutions modulo $\mathfrak{p}^{n+1}$, and in fact to solutions in $\mathfrak{o}^d$.

Note that if x is a solution modulo $\mathfrak{p}^n$ with $n \geq 2N + 1$ then so are all $x + \varpi^{n-N}h$, since then

$$f(x + \varpi^{n-N}h) \equiv_n f(x_n) + \varpi^{n-N+N}\langle \nabla_f(x), h\rangle \equiv_n f(x_n) .$$

I think the final result is this: say there are M solutions modulo $\mathfrak{p}^{N+1}$ that come from solutions modulo $\mathfrak{p}^{2N+1}$. Then these lift to $\mathfrak{o}$, and more generally modulo $\mathfrak{p}^{N+1+n}$ there are $Mq^{(d-1)k}$ solutions that lift to $\mathfrak{o}$. This at least agrees with what happens in the non-singular case, in which $N = 0$ and any non-singular solutions over $\mathbb{F}_q$ lift to $\mathfrak{o}$.

For example, take $f(x) = x^2 - 17$ and $\mathfrak{o} = \mathbb{Z}_2$. Then $\nabla_f = 2x$. Any solution of $f(x) = 0$ will be a unit, so $N = 1$. Each of the four units x in $\mathbb{Z}_8$ is a solution of $f(x) \equiv_3 a$, and for any of them we may find y in $\mathbb{Z}/16$ with $y \equiv_2 x$. Modulo 16 there are again 4 solutions, whose images modulo 8 are half the solutions modulo 8. Etc. In general, half the solutions in $\mathbb{Z}/p^n$ lift to solutions in $\mathbb{Z}_p$. They are the ones that lift to solutions in $\mathbb{Z}/p^{n+1}$.

If f is a system of equations then ∇_f is a matrix, to which we must presumably apply the principal divisor theorem, assuming the point is *not* singular over $\mathfrak{k}$, but only singular to finite depth over $\mathfrak{o}$. Thus ∇_f is a matrix of maximum rank over $\mathfrak{k}$, and to apply the same reasoning as above we must express lattices accordingly.

[hensels-theorem-2] **3.2. Theorem.** *Suppose x_n satisfies*

$$f(x_n) \equiv_n 0, \quad \nabla_f(x) \equiv_N 0, \quad \nabla_f(x) \not\equiv_{N+1} 0 .$$

If $n \geq 2N + 1$, there exists x in $\mathfrak{o}^d$ with $f(x) = 0$ and $x \equiv_{n-N} x_n$.