11:44 a.m. April 2, 2011

# Hensel's Lemma

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

The general question is: *Suppose $V$ an algebraic variety defined over $\mathbb{Z}_p$. What can one say about the number of points defined over $\mathbb{Z}p^m$, as $m$ grows?* Hensel's Lemma answers this question when $V$ is non-singular as a variety over $\mathbb{Q}_p$.

Given $\mathfrak{k}$, $\mathfrak{o}$, $\mathfrak{p} = (\varpi)$, $\mathbb{F}_q = \mathfrak{o}/\mathfrak{p}$. Let $\equiv_n$ mean congruence modulo $\mathfrak{p}^n$.

**Contents**



## 1. Introduction

Let's look at the simplest case, with $f(x) = x^2 - 1$.

Suppose first that $p$ is odd. There are two solutions modulo $p$. What about modulo $p^n$? We proceed by induction. Suppose that we know all solutions modulo $p^n$ and want to find all those modulo $p^{n+1}$. If $x$ is a solution modulo $p^{n+1}$ its image modulo $p^n$ is also a solution, What is the inverse image of a solution in $\mathbb{Z}/p^n$? We may take $x$ to be any element of $\mathbb{Z}/p^{n+1}$ such that $x^2 \equiv_n 1$. So We want to find all $ep^n$ for which

$$(x + ep^n)^2 = x^2 + 2ep^n + e^2p^{2n} \equiv_{n+1} 1\,.$$

Since $n \geq 1$, the last term lies in $p^{n+1}$, so we may ignore it. But then we may set

$$e = \frac{1 - x^2}{2x}\,,$$

which is legitimate because $2x$ is invertible in $\mathbb{Z}/p$. As I said, we are looking at the $p$-adic Newton's method of finding roots. The point here is that $e$ is unique modulo $p$, hence $ep^n$ unique modulo $p^{n+1}$. So (as we knew already) there are exactly two square roots of $1$ in $\mathbb{Z}_p$ if $p$ is odd.

The case $p = 2$ is more interesting. There is one solution in $\mathbb{Z}/p$, 2 in $\mathbb{Z}/4$, four solutions in $\mathbb{Z}/8$, and $4$ in $\mathbb{Z}/16$. Does this number remain fixed for $n \geq 3$? Yes, but for slightly peculiar reasons. 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 $\pm 1$, $\pm 7$—i.e. only half the units. Their images in $\mathbb{Z}/8$ give only $\pm 1$, which is to say that only half the solutions in $\mathbb{Z}/*$ 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 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 $2x$ is no longer a unit, so in order to make it work the numerator has to be more divisible by 2.

In the next section I'll deal with Hensel's Lemma in the case that generalizes what happened for $x^2 - 1$ when $p$ was odd, and in the section after that I'll deal with the singular cases.

## 2. The simplest case

I shall look in this section and the next at the case when the variety is a hypersurface $f = 0$, generically non-singular, which is to say over $\mathbb{Q}_p$. I recall that the scheme $f = 0$, in which $f$ has coefficients in the field $F$, is non-singular if its gradient never vanishes identically at its $F$-rational points. I shall assume in this section that $f = 0$ remains non-singular modulo $p$. First a very local result:

[hensel] **Theorem 2.1.** (Hensel's Lemma I.) *Suppose $f(x)$ a polynomial in $d$ variables with coefficients in $\mathfrak{o}$ such that $\nabla f(x)$ is non-zero modulo $p$. Then for every solution $x_n$ of $f(x_n) \equiv_n 0$ there exist $p^{d-1}$ solutions modulo $\mathfrak{p}^{n+1}$ that are $\equiv_n x_n$.*

This is precisely the statement we mst need to to make sense of Siegel's formula.

*Proof.* I do the case $N = 0$ first, partly because it is the most commonly applied case, partly because it is simpler to state and to prove. The assumption means that $\nabla f(x_0)$ 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 $f(x_n) \equiv_n 0$ with $x_n \equiv_1 x_0$ 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

$$f(x + \varpi^n a) = f(x) + \varpi^n \langle \nabla f(x_0), a \rangle \equiv_{n+1} 0$$

by solving $\langle \nabla f(x_0), a \rangle = -f(x_n)/\varpi^n$.

## 3. When f=0 is singular modulo p

Now suppose $N$ arbitrary. Given $x_n$, any $x_n + \varpi^{n-N} a_n$ will also be a solution, with $a_n \in (\mathfrak{o}/\mathfrak{p}^N)^d$. That gives us precisely $q^N$ solutions all equal modulo $\varpi^{n-N}$. Chosoe $x \equiv_n x_n$, and consider $x + \varpi^{n-N} a$. We have

$$f(x + \varpi^{n-N} a) = f(x) + \langle \nabla f(x), \varpi^{n-N} a \rangle + O(\varpi^{2(n-N)})$$

Under the assumption $n \geq 2N + 1$, this last is $O(\varpi^{n+1})$, so we can ignore it. But $f(x) = \varpi^n y$, $\nabla f(x) = \varpi^N v$, $v \not\equiv_1 0$, so the remainder is $\varpi^n y + \varpi^{n-N} \varpi^N \langle v, a \rangle$, which we may solve for $q^{d-1}$ values of $a$.

So we get for each equivalence class of $q^N$ solutions modulo $\varpi^n$ a set of $q^N q^{d-1}$ solutions modulo $\varpi^{n+1}$. ∎

As a simple example, consider the equation $x^2 = 1$ in $\mathbb{Z}_2$. Here $d = 1$, $N = 2$, and $2N + 1 = 3$. There are $4$ solutions of $x^2 \equiv 1$ modulo $8$. The theorem asserts that there are $4$ modulo $2^n$ for all $n \geq 3$.

If $f$ is a system of equations then $\nabla f$ is a matrix, to which we presumably apply the principal divisor theorem: assuming the point is *not* singular over $\mathfrak{k}$, but only singular to finite depth. Thus $\nabla f$ is a matrix of maximum rank.

**Exercise 1.** *Formulate and prove a version of Hensel's Lemma that explains under what conditions a system of $m$ equations*

$$f_i(x_1, \ldots, x_n) = 0$$

*has the property that for every solution $x_n$ modulo $\mathfrak{p}^n$ there exist exactly $q^{n-m}$ solutions $x_{n+1} \equiv_n x_n$.*

**Exercise 2.** *How many solutions $X$ of*

$${}^t X I X \equiv 1$$

*are there modulo every $2^k$?*