Lecture 5.

14.07.2011.

Hensel's Lemma III. Let $f(x) \in \mathbb{Z}_p[x]$

Suppose $\alpha_0 \in \mathbb{Z}_p$ s.t.

$|f'(\alpha_0)|_p^2 > |f(\alpha_0)|_p$ (i.e. if $p^n \| f(\alpha_0)$, $p^m \| f'(\alpha_0)$, then $n > 2m$)

Then there exists $\alpha \in \mathbb{Z}_p$ s.t: $f(\alpha) = 0$

$|\alpha - \alpha_0|_p \le p^{-r}$, $r = \mathrm{ord}_p(f(\alpha_0)/f'(\alpha_0))$

$|f'(\alpha)|_p = |f'(\alpha_0)|_p$ (in fact, α is unique)

Proof Essentially the same.

Take more care with powers of p

(most easily expressed in terms of $|\cdot|_p$)

α is the limit $\alpha_{n+1} = \alpha_n - f(\alpha_n)/f'(\alpha_n)$

Example where this is useful:

$3x^3 + 4y^3 = 5$ has solution in $\mathbb{Q}_p$ for all p.

Claim: there exists $y \in \mathbb{Q}_3$

s.t. $4y^3 = 5$

$y = 2$ solution to $4y^3 - 5 \equiv 0 \ (3^3)$

$+ \quad |3 \cdot 4(2^2)|_3 = 3^{-1}$

so can apply HLIII.

Quadratic forms $/\mathbb{Q}_p$.

$$F(x_1, \dots, x_s) = \sum_{1 \le i,j \le s} c_{ij} x_i x_j, \quad c_{ij} = c_{ji}$$

Thm If $s \ge 5$ then there exists

$0 \ne \underline{a} \in \mathbb{Q}_p^s$ s.t. $F(\underline{a}) = 0$

Pf (for $p \ne 2$)

$$F(x_1, \dots, x_s) = (x_1, \dots, x_s)(c_{ij})\begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix}$$

Make a change of variable that diagonalizes the matrix (c_{ij})

so we are really looking at

$$c_1 x_1^2 + c_2 x_2^2 + \dots + c_s x_s^2 = 0, \quad c_i \in \mathbb{Q}_p, \ \prod_i c_i \ne 0$$

write $c_i = p^{k_i} a_i$, $a_i \in \mathbb{Z}_p^\times$, $k_i \in \mathbb{Z}$.

$p^{2n} = (p^n)^2$

$I_j = \{ i \in \{1, \dots, s\} : k_i \equiv j \ (2) \}$ $j = 0, 1$

$$\sum_{i\in I_0} a_i \underbrace{(p^{k_i/2} x_i)^2}_{y_i} + p \sum_{i \in I_1} a_i \underbrace{(p^{\frac{k_i-1}{2}} x_i)^2}_{y_i}$$

$$\sum_{i\in I_0} a_i y_i^2 = 0 \qquad \sum_{i\in I_1} a_i y_i^2 = 0$$

If $s \geq 5$ some I_j has size at least 3:

$$\sum_{i \in I_j} a_i y_i^2 = 0$$

By Chevalley-Warning:

$|I_j| \geq 3 > 2 \Rightarrow$ there exists a non-zero solution modulo p.

$\Leftarrow$ p-odd since $a_i \in \mathbb{Z}_p^*$

By Hensel's lemma I, II there exists a non-zero solution in $\mathbb{Q}_p$

Thm: If $s > d^2+1$ and $p \nmid d$ then any equation

$$c_1 x_1^d + \dots + c_s x_s^d = 0 \qquad c_i \in \mathbb{Q}_p$$

has a non-zero solution in $\mathbb{Q}_p$ (still ~~have~~ true if pl

Thm (of Brower). Let $d \geq 1$

There exist~~s~~ any integer $\varphi(d) > 0$ s.t if $F(x_1, .., x_n)$ is a homogeneous equation of degree d in $n \geq \varphi(d)$ variables, there $F(\underline{x}) = 0$ has a non-zero solution in $\mathbb{Q}_p$.

($\varphi(d)$ exists indep. of p)

(If $d=3$, then $\varphi(d) = 10$).

$d=3$ Either there exists a zero of

$$F(\underline{x}) = a x_1^3 + Q(x_2, .., x_n) x_1^1 + L(x_2, .., x_n) x_1^2 + C(x_2, .., x_n)$$

Proposition Let $F(x_1, .., x_s)$ be a quadratic form with $c_{ij} \in \mathbb{Z}_p$.

If there exists a solution to

$$F(\underline{x}) \equiv 0 \mod p^r$$

with $r = 2\,\mathrm{ord}_p(2\det(c_{ij})) + 1$

and some $x_i \not\equiv 0 \pmod p$

then there is non-zero solution in $\mathbb{Q}_p$

- can talk about continuous functions

$f: \mathbb{Z}_p \to \mathbb{Q}_p$

or $\mathbb{Q}_p \to \mathbb{Q}_p$

continuous at y:

Given $\varepsilon > 0$ there exist $\delta > 0$

s.t. if $|x-y|_p < \delta$

then $|f(x)-f(y)|_p < \varepsilon$

$$\binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!}$$

If $x \in \mathbb{N}$, then $\binom{x}{n} \in \mathbb{Z}$

If $x \in \mathbb{Z}_p$, then $\binom{x}{n} \in \mathbb{Z}_p$

Thm (Mahler) If $f: \mathbb{Z}_p \to \mathbb{Q}_p$ is a continuous function then

$$f(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m}, \quad |a_m|_p \to 0$$

Thm (Skolem)

Let $a_{n+2} = A a_{n+1} + B a_n$, $A, B \in \mathbb{Z}$ be a recurisine sequence.

Either

(i) $\{a_n\}$ is eventually periodic

(ii) a_n takes us any given value at most finites many tines.

($a_n = x$ for only finitely many n).

idea $\quad x^2 - Ax + B = (x-\alpha)(x-\beta)$

$$a_n = C\alpha^n + D\beta^n, \quad C, D \in \mathbb{Q}$$

$$\alpha = \frac{A + \sqrt{A^2-4B}}{2} \qquad \beta = \frac{A - \sqrt{A^2-4B}}{2}$$

$$\alpha^n = \frac{1}{2^n} \sum_{j=0}^{n} A^j \sqrt{A^2-4B}^{\,n-j} \binom{n}{j}$$

$$a_n = \sum_{m=0}^{\infty} b_m \binom{n}{2m} (A^2-4B)^m$$

$x^2 + 7 = 2^n$ for finitely many n

$n = 3, 4, 5, 7, 15$

$$\frac{x^2+7}{4} = \left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)$$

$$2 = \left(\frac{1+\sqrt{-7}}{2}\right)\left(\frac{1-\sqrt{-7}}{2}\right)$$

$$\frac{x+\sqrt{-7}}{2} = \pm\left(\frac{1+\sqrt{-7}}{2}\right)^n \text{ or } \pm\left(\frac{1-\sqrt{-7}}{2}\right)^n$$

$$\frac{a_n + b_n\sqrt{-7}}{2} \quad ?\ b_n = \pm 1$$