Formal groups and congruences

Masha Vlasenko

June 30, 2016
Porquerolles

Formal group laws

R commutative ring with 1
$F(x,y) \in R[\![x,y]\!]$ formal group law of dimension 1 over R

$$\begin{aligned} F(x,0) &= F(0,x) = x \\ F(F(x,y),z) &= F(x,F(y,z)) \end{aligned}$$

homomorophisms

$$R' \supseteq R\,, \qquad h \in \mathrm{Hom}_{R'}(F_1,F_2)\ :$$
$$h(x) = u_1 x + u_2 x^2 + \ldots \in R'[\![x]\!]$$
$$h(F_1(x,y)) = F_2(h(x),h(y))$$

$u_1 \in (R')^\times$ isomorphism
$u_1 = 1$ strict isomorphism

The logarithm of a formal group law

assume: $R \to R \otimes \mathbb{Q}$ is injective (characteristic 0 ring)
then:

$$\begin{aligned} \exists! \quad f(x) \;&=\; x + \ldots \;\in\; \mathrm{Hom}_{R\otimes\mathbb{Q}}(F, \mathbb{G}_a) \\ \Leftrightarrow F(x,y) \;&=\; f^{-1}(f(x) + f(y)) \end{aligned}$$

Construction:

$$\log_F(x) := f(x) \;=\; \int dx \Big/ \frac{\partial F}{\partial x}(0,x)$$

Example:

$$\begin{aligned} F(x,y) \;&=\; x + y + c\,xy \\ f(x) \;&=\; \int \frac{dx}{1+cx} \;=\; \int \sum_{n=0}^{\infty} (-cx)^n \, dx \;=\; \sum_{n=1}^{\infty} (-c)^{n-1} \frac{x^n}{n} \end{aligned}$$

Constructing $f(x) = \log_F(x)$

$$(i) \quad F(x,0) \;=\; F(0,x) \;=\; x \qquad (ii) \quad F(F(x,y),z) \;=\; F(x,F(y,z))$$

$$(i) \;\Rightarrow\; \frac{\partial F}{\partial x}(0,x) \in 1 + xR[\![x]\!]\,, \quad g(x) := 1/\frac{\partial F}{\partial x}(0,x)$$

$$\frac{\partial}{\partial x}(ii) \;:\; \frac{\partial F}{\partial x}(F(x,y),z) \cdot \frac{\partial F}{\partial x}(x,y) \;=\; \frac{\partial F}{\partial x}(x,F(y,z))$$

$$(x,y,z) = (0,x,y) : \; \frac{\partial F}{\partial x}(x,y) \cdot \frac{\partial F}{\partial x}(0,x) \;=\; \frac{\partial F}{\partial x}(0,F(x,y))$$

$$g(F(x,y)) \cdot \frac{\partial F}{\partial x}(x,y) \;=\; g(x)$$

$$f(x) := \int g(x)dx : \; \frac{\partial}{\partial x} f(F(x,y)) \;=\; \frac{\partial}{\partial x} f(x)$$

$$\frac{\partial}{\partial x}\Big(f(F(x,y)) - f(x)\Big) \;=\; 0$$

$$f(F(x,y)) \;=\; f(x) + h(y)$$

$$x = 0, y = x : \; h(x) \;=\; f(x) \;\Rightarrow\; f(F(x,y)) \;=\; f(x) + f(y)$$

Part I: integrality

$$F \in R[\![x,y]\!] \quad \rightsquigarrow \quad \begin{aligned} F(x,y) &= f^{-1}(f(x)+f(y)) \\ f(x) &= \int dx \Big/ \frac{\partial F}{\partial x}(0,x) \in (R \otimes \mathbb{Q})[\![x]\!] \\ f(x) &= \sum_{n=1}^{\infty} b_{n-1} \frac{x^n}{n} \\ b_0 &= 1, b_1, b_2, \ldots \in R \end{aligned}$$

Goal: Characterize sequences $\{b_n; n \geq 0\}$ that occur in the above construction.

p-transform

assume: $\exists\,\sigma \in \mathrm{End}(R) \quad : \quad \sigma(a) \equiv a^p \mod pR \quad \forall\, a \in R$

$$\{b_n; n \geq 0\} \leftrightsquigarrow \{c_n; n \geq 0\}$$

$$b_n = c_n + \sum_{n=m*k} c_m \cdot \sigma^{\ell(m)}(b_k) \qquad m*k = m + k\,p^{\ell(m)}$$

$$\ell(m) = \min\{s \geq 1 : m < p^s\}$$

$$c_0 = b_0\,, \quad c_1 = b_1\,, \quad \ldots\,, \quad c_{p-1} = b_{p-1}\,,$$
$$c_p = b_p - b_0\,\sigma(b_1)\,, \quad c_{1+p} = b_{1+p} - b_1\,\sigma(b_1)\,, \quad \ldots$$
$$c_{p^2} = b_{p^2} - b_0\,\sigma(b_p)\,, \quad c_{1+p^2} = b_{1+p^2} - b_1\,\sigma(b_p)\,, \quad \ldots$$
$$c_{p+p^2} = b_{p+p^2} - b_0\,\sigma(b_{1+p}) - b_p\,\sigma^2(b_1) + b_0\,\sigma(b_1)\sigma^2(b_1)\,, \quad \ldots$$

Criterion of integrality

$$f(x) = \sum_{n=1}^{\infty} b_{n-1} \frac{x^n}{n}$$

$$b_0 = 1, b_1, b_2, \ldots \in R \quad \rightsquigarrow \quad \{c_n; n \geq 0\} \quad p\text{-sequence}$$

Theorem 1. (MV, Eric Delaygue)
$F(x,y) = f^{-1}(f(x) + f(y)) \in (R \otimes \mathbb{Z}_{(p)})[\![x,y]\!]$
$\Leftrightarrow$
the p-sequence $\{c_n; n \geq 0\}$ associated to $\{b_n; n \geq 0\}$ satisfies

$$c_{mp^k-1} \in p^k R \quad \text{for all} \quad m > 1, k \geq 0$$

Idea of proof: Hazewinkel's functional equation lemma

$$\text{if } \exists\, v_1, v_2, \ldots \in R \text{ s.t. } f(x) - \frac{1}{p}\sum_{i=1}^{\infty} v_i \cdot \sigma^i(f)(x) \in R[\![x]\!]$$

$$\text{then } F(x,y) = f^{-1}(f(x) + f(y)) \in R[\![x]\!]$$

conversely:
if R is a $\mathbb{Z}_{(p)}$-algebra then every formal group law over R is *of functional equation type*

Proof of Theorem 1: the obvious direction

$$c_{mp^k-1} \in p^k R \quad \text{for all} \quad m > 1, k \geq 0$$

$$\Downarrow$$

$$v_i := \frac{1}{p^{i-1}} c_{p^i-1} \in R \qquad i = 1, 2, \ldots$$

$$\sum_{n=1}^{\infty} d_n x^n := f(x) - \frac{1}{p} \sum_{i=1}^{\infty} v_i \cdot (\sigma^i f)(x)$$

$$(n = mp^k) \quad d_n = \frac{1}{mp^k} b_{mp^k-1} - \frac{1}{p} \sum_{i=1}^{k} v_i \cdot \frac{1}{mp^{k-i}} \sigma^i (b_{mp^{k-i}-1})$$

$$= \frac{1}{mp^k} \left(b_{mp^k-1} - \sum_{i=1}^{k} c_{p^i-1} \cdot \sigma^i (b_{mp^{k-i}-1}) \right)$$

$$= \frac{1}{mp^k} \sum_{m=m' * m''} c_{m'p^k-1} \cdot \sigma^{k+\ell(m')} (b_{m''}) \in R \otimes \mathbb{Z}_{(p)}$$

Functional Equation Lemma $\Rightarrow F(x, y) \in (R \otimes \mathbb{Z}_{(p)})[\![x, y]\!]$

Proof of Theorem 1

$$F(x,y) \in (R \otimes \mathbb{Z}_{(p)})[\![x,y]\!] \;\Rightarrow\; \exists v_1, v_2, \ldots \in R \otimes \mathbb{Z}_{(p)} \text{ s.t.}$$

$$\sum_{n=1}^{\infty} d_n x^n := f(x) - \frac{1}{p} \sum_{i=1}^{\infty} v_i \cdot (\sigma^i f)(x) \in (R \otimes \mathbb{Z}_{(p)})[\![x]\!]$$

$$c_{p^k-1} \;=\; p^{k-1} v_k + p^k d_{p^k} - \sum_{i=1}^{k-1} \sigma^i(c_{p^{k-i}-1})\, p^i\, d_{p^i} \in p^{k-1} R$$

$$\widetilde{f}(x) - \frac{1}{p} \sum_{s=1}^{\infty} v_s \cdot (\sigma^s \widetilde{f})(x) \;=\; \sum_{k=0}^{\infty} d_{p^k}\, x^{p^k}\,, \qquad \widetilde{F}(x,y) \cong F(x,y)$$

$$\widetilde{f}(x) - \frac{1}{p} \sum_{i=1}^{\infty} v'_i \cdot (\sigma^i \widetilde{f})(x) \;=\; x\,, \qquad v'_i \;:=\; \frac{1}{p^{i-1}} c_{p^i-1} \;\in R$$

$$f(x) - \frac{1}{p} \sum_{i=1}^{\infty} v'_i \cdot (\sigma^i \widetilde{f})(x) \in (R \otimes \mathbb{Z}_{(p)})[\![x]\!] \;\Rightarrow\; c_{mp^k-1} \in p^k R \quad \square$$

Example 1: formal group laws from L-functions

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \mathcal{P}_p(p^{-s})^{-1} \qquad \mathcal{P}_p(T) \in 1 + T\mathbb{Z}[T]$$

$$F(x,y) = f^{-1}(f(x) + f(y)), \qquad f(x) = \sum_{n=1}^{\infty} \frac{a_n}{n} x^n$$

Corollary (of Theorem 1):

$$F(x,y) \in \mathbb{Z}_{(p)}[\![x,y]\!] \quad \Leftrightarrow \quad \mathcal{P}_p(T) = 1 + \sum_{i=1}^{d} \gamma_i T^i \ \text{ with } \ p^{i-1} | \gamma_i$$

Lemma

$$a_1 = 1\,,\ a_2, a_3, \ldots \in \mathbb{Z}$$

$$\{b_n := a_{n+1}; n \geq 0\} \quad \rightsquigarrow \quad \{c_n; n \geq 0\} \quad (p\text{-sequence})$$

Then:

- $a_{mp^k} = a_m a_{p^k}$ for all $k \geq 0$, $p \not| m$
  $\Leftrightarrow \quad c_{mp^k-1} = 0$ for all $k > 0$, $p \not| m$, $m > 1$
- $\exists\, d \geq 0$ and $\gamma_1, \ldots, \gamma_d \in \mathbb{Z}$ s.t.

$$a_{p^k} + \gamma_1\, a_{p^{k-1}} + \ldots + \gamma_m\, a_{p^{k-m}} = 0 \quad \text{for all } k \geq 0$$

$\Leftrightarrow$

$$c_{p^i-1} = \begin{cases} -\gamma_i\,, & 1 \leq i \leq d\,, \\ 0\,, & i > d\,. \end{cases}$$

Example 2: formal group laws from polynomials

$H(\underline{X}) \in R[X_1^{\pm 1}, \ldots, X_N^{\pm 1}]$ $\quad \Delta(H) \subset \mathbb{R}^N$ Newton polytope

assume: $\Delta(H)^\circ \cap \mathbb{Z}^N = \{\underline{u}\}$ (unique internal integral point)

$$F(x,y) = f^{-1}(f(x) + f(y))\,, \qquad f(x) = \sum_{n=1}^{\infty} \frac{b_{n-1}}{n}\, x^n$$

$b_n :=$ coefficient of $\underline{X}^{n\underline{u}}$ in $H(\underline{X})^n$

$\forall p \quad \rightsquigarrow \quad \{c_n ; n \ge 0\}$ satisfies $c_n \in p^{\ell(n)-1} R$ (A.Mellit, 2009)

Theorem 1 $\Rightarrow$ $\qquad F(x,y) \in R[\![x,y]\!]$

Remark: if $V = \{H(\underline{X}) = 0\} \subset \mathbb{P}^{N-1}$, smooth, then $F(x,y)$ is a coordinalization of the Artin-Mazur formal group $H^{N-2}(V, \hat{\mathbb{G}}_{m,V})$ (J. Stienstra, 1987)

Part II: p-adic formulas for local invariants

$G(x,y) \in \mathbb{F}_p[\![x,y]\!]$

$[p]_G \in \mathrm{End}_{\mathbb{F}_p}(G)$ 'multiplication by p' endomorphism

$$[p]_G(x) \;:=\; \underbrace{x \;+_G x \;+_G \ldots \;+_G x}_{p} \;=\; G(x, G(x, \ldots G(x,x\underbrace{) \ldots))}_{p}$$

$\phi(x) \;=\; x^p \in \mathrm{End}_{\mathbb{F}_p}(G)$ Frobenius endomorphism

$h_G := \sup\{m \;:\; [p]_G(x) \in \mathbb{F}_p[\![x^{p^m}]\!]\}$ height

Theorem. $\mathrm{End}_{\mathbb{F}_p}(G)$ is a $\mathbb{Z}_p$-algebra and ϕ satisfies an irreducible polynomial equation over $\mathbb{Z}_p$ of degree $h = h_G$:

$$p + \alpha_1\phi + \alpha_2\phi^2 + \ldots + \alpha_h\phi^h = 0\,,$$

where $\alpha_1, \ldots, \alpha_{h-1} \in p\mathbb{Z}_p$, $\alpha_h \in \mathbb{Z}_p^\times$.

Theorem 2. (MV) Let $F \in \mathbb{Z}[\![x,y]\!]$ be a formal group law of dimension 1 with $\log_F(x) = \sum_{n=1}^{\infty} b_{n-1} \frac{x^n}{n}$. Let

$$\overline{F} = F \mod p\,, \quad h_p = h_{\overline{F}} \ \textit{height at } p$$

$$\Psi_p(T) = p + \alpha_1 T + \ldots + \alpha_h T^h \ \textit{char. polynomial at } p$$

Then:

- $\mathrm{ord}_p(b_{p^n-1}) \geq n - \lfloor \frac{n}{h} \rfloor$ with equality when $h|n$
- numbers $\beta_n := b_{p^n-1}/p^{n-\lfloor \frac{n}{h} \rfloor} \in \mathbb{Z}$ satisfy $\beta_{kh} \equiv \beta_h^k \mod p\,, \forall k$
- for $k \geq 1$ define $h \times h$ matrices

$$D_k := \left(p^{\varepsilon_{ij}} \beta_{kh-1+i-j}\right)_{0 \leq i,j \leq h-1} \quad \varepsilon_{ij} = \begin{cases} 0\,, & j < i \text{ or } j = h-1 \\ 1\,, & i \leq j < h-1 \end{cases}$$

We have $\det D_k \equiv (-1)^{h-1} \beta_h^{kh-1} \neq 0 \mod p$ and

$$-D_k^{-1} \begin{pmatrix} \beta_{kh} \\ \beta_{kh+1} \\ \vdots \\ \beta_{kh+h-2} \\ \beta_{kh+h-1} \end{pmatrix} \equiv \begin{pmatrix} \alpha_1/p \\ \alpha_2/p \\ \vdots \\ \alpha_{h-1}/p \\ \alpha_h \end{pmatrix} \mod p^k\,.$$

Theorem 2: p-adic formulas for local invariants

- $h_p = 1$: $\quad p \nmid b_{p^k-1} \quad \forall k$

$$\Psi_p(T) = p + \alpha_1 T$$
$$\alpha_1 \equiv -b_{p^k-1}/b_{p^{k-1}-1} \mod p^k$$

- $h_p = 2$: $\quad \nu_p(b_{p^{2k}-1}) = k \quad \nu_p(b_{p^{2k-1}-1}) \geq k \quad \forall k$

$$\Psi_p(T) = p + \alpha_1 T + \alpha_2 T^2$$

$$\begin{pmatrix} \frac{\alpha_1}{p} \\ \alpha_2 \end{pmatrix} \equiv -\begin{pmatrix} p\,\frac{b_{p^{2k-1}-1}}{p^k} & \frac{b_{p^{2k-2}-1}}{p^{k-1}} \\ \frac{b_{p^{2k}-1}}{p^k} & \frac{b_{p^{2k-1}-1}}{p^k} \end{pmatrix}^{-1} \begin{pmatrix} \frac{b_{p^{2k}-1}}{p^k} \\ \frac{b_{p^{2k+1}-1}}{p^{k+1}} \end{pmatrix} \mod p^k$$

Idea of proof: formal Weierstrass preparation lemma

$f(x) = \log_F(x) \qquad \exists \quad v_1, v_2, \ldots \in \mathbb{Z}_{(p)} \qquad$ s.t.

$$f(x) - \frac{1}{p}\sum_{s=1}^{\infty} v_s\,(\sigma^s f)(x) \in \mathbb{Z}_{(p)}[\![X]\!]$$

Lemma
$h_p \;=\; \inf\{s \geq 1 \;:\; v_s \in \mathbb{Z}_p^\times\}$

Lemma (Taira Honda, 1960's)
$\exists! \quad \theta(T) \in \mathbb{Z}_p[\![T]\!]^\times$ and $\alpha_1, \ldots, \alpha_{h-1} \in p\mathbb{Z}_p$, $\alpha_h \in \mathbb{Z}_p^\times$ s.t.

$$\theta(T)\Big(p - \sum_{s=1}^{\infty} v_s T^s\Big) \;=\; p + \sum_{i=1}^{h} \alpha_i T^i$$

Example 1: formal group laws from L-functions

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \mathcal{P}_p(p^{-s})^{-1} \qquad \mathcal{P}_p(T) \in 1 + T\mathbb{Z}[T]$$

$$\mathcal{P}_p(T) = 1 + \sum_{i=1}^{d} \gamma_i T^i \text{ with } p^{i-1} | \gamma_i \qquad \Leftrightarrow$$

$$Q_p(T) := p\,\mathcal{P}_p\left(\frac{T}{p}\right) \in p + T\,\mathbb{Z}[T] \quad \rightsquigarrow \quad F(x,y) \in \mathbb{Z}_{(p)}[\![x,y]\!]$$

By Theorem 2:

$$h_p = \text{ the highest power of } T \text{ that divides } \overline{Q}_p = Q_p \mod p$$

$$\Psi_p(T) = \text{ the unique Eisenstein factor of } Q_p(T)$$

Example 2: Artin-Mazur formal group laws

$H(X) \in R[X_1^{\pm 1}, \dots, X_N^{\pm 1}]$ $\quad \Delta(H) \subset \mathbb{R}^N$ Newton polytope

assume: $\Delta(H)^\circ \cap \mathbb{Z}^N = \{u\}$ (unique internal integral point)

$b_n :=$ coefficient of X^{nu} in $H(X)^n$ $\quad f(x) = \sum_{n=1}^{\infty} \frac{b_{n-1}}{n} x^n$

$F(x,y) = f^{-1}(f(x) + f(y)) \in R[\![x,y]\!]$ is a coordinalization of the Artin-Mazur formal group $H^{N-1}(V, \hat{\mathbb{G}}_{m,V})$

$V \subset \mathbb{P}^N$ is a non-singular compactification of $\{H(X) = 0\}$

assume: $R = \mathbb{Z}$, $\mathcal{V} = V \times_{Spec\,\mathbb{Z}} Spec\,\mathbb{F}_p$ is non-singular
$\Rightarrow$ the Cartier module of the Artin–Mazur formal group is isomorphic to the de Rham–Witt cohomology $H^{N-1}(\mathcal{V}, W\mathcal{O}_{\mathcal{V}})$

Artin-Mazur formal group laws

Corollary:

$$h_p = 1 \quad \Leftrightarrow \quad \exists!\, \lambda_p \ \text{ the } p\text{-adic unit eigenvalue of the Frobenius operator on the middle crystalline cohomology}$$

$$\Psi_p(T) \;=\; p - \lambda_p T \qquad \lambda_p \;=\; \lim_{s\to\infty} \frac{b_{p^s-1}}{b_{p^{s-1}-1}}$$

Example. $V \;=\; \{X_1^N \,+\, X_2^N \,+\, \ldots \,+\, X_N^N \;=\; 0\}$

$$b_n \;=\; \text{coefficient of } (X_1 X_2 \ldots X_N)^n \text{ in } (X_1^N + X_2^N + \ldots + X_N^N)^n$$
$$= \begin{cases} 0\,, & \text{if } N \nmid n\,, \\ n!/(n/N)!^N\,, & \text{if } N \mid n\,. \end{cases}$$

Example: Fermat's hypersurface $X_1^N + X_2^N + \ldots + X_N^N = 0$

$$b_n = \text{coefficient of } (X_1 X_2 \ldots X_N)^n \text{ in } (X_1^N + X_2^N + \ldots + X_N^N)^n$$
$$= \begin{cases} 0\,, & \text{if } N \nmid n \\ n!/(n/N)!^N\,, & \text{if } N \mid n \end{cases}$$

By Theorem 2:

$$h_p = \begin{cases} 1\,, & \text{when } p \equiv 1 \mod N \\ 2\,, & \text{when } N = 3\,,\ p \equiv -1 \mod 3 \\ \infty\,, & \text{otherwise} \end{cases}$$

for all $p \equiv 1 \mod N$:
the p-adic unit eigenvalue of Frobenius on $H^{N-2}_{crys}(\mathcal{V})$ is given by

$$\lambda_p \mod p^n \equiv \frac{b_{p^n-1}}{b_{p^{n-1}-1}} = \frac{(p^n-1)!}{(p^{n-1}-1)!} \cdot \left(\frac{\left(\frac{p^n-1}{N}\right)!}{\left(\frac{p^{n-1}-1}{N}\right)!}\right)^{-N} = \frac{\Gamma_p(p^n)}{\Gamma_p\left(\frac{p^n-1}{N}+1\right)^N}$$

$$\lambda_p = \frac{\Gamma_p(0)}{\Gamma_p(1-\frac{1}{N})^N} = \Gamma_p(1-\frac{1}{N})^{-N} = (-1)^N\,\Gamma_p(\frac{1}{N})^N$$

thank you