Beyond elliptic cohomology and TMF: where number theory and stable homotopy theory meet in mortal combat.

University of Rochester
Topology Seminar

Doug Ravenel

March 10, 2006

1. Introduction

This talk is an ad for a course I plan to give next fall about the mathematics surrounding the research I have been doing for the past 3 years. It might be called "Applications of arithmetic algebraic geometry to stable homotopy theory." Its syllabus might look like this.

- Motivation from stable homotopy theory: how an intimate knowledge of formal groups leads to insights about the stable homotpy groups of spheres.
- Relevant methods from algebraic geometry: how algebraic curves lead to interesting and useful examples of formal groups.
- Lubin-Tate's theory of deformations of formal groups.
- Explicit computations involving the Lagrange inversion formula and Honda matrices.

For today I will give a taste of this by describing some results about the following question.

> What is the formal group associated with the Jacobian of an algebraic curve defined over the p-adic integers?

Do not worry if you do not know what these words mean!

2. Formal group laws

Let G be an n-dimensional commutuative analytic Lie group and suppose we have a local coordinates $\{x_1, x_2, \ldots, x_n\}$ for which the origin is the identity element. Then the multiplication map $G \times G \to G$ can be described by n power series in $2n$ variables

$$F_i(x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n) \qquad \text{for } 1 \leq i \leq n.$$

We will often abbreviate this by $F(x, y)$, where x, y and F are understood to be n-dimensional vectors. F must satisfy the following conditions.

(i) $F(x, 0) = F(0, x) = x$ (The origin is the identity element)

(ii) $F(F(x, y), z) = F(x, F(y, z))$ (Associativity)

(iii) $F(x, y) = F(y, x)$ (Commutativity)

(i) implies $F(x, y) \equiv x + y$ modulo xy, and the existence of inverses (a vector of power series $i(x)$ with $F(x, i(x)) = 0$) follows from the implicit function theorem.

Definition 1. *An n-dimensional commutative formal group law over a commutative ring R is a collection of n power series*

$$F_i(x, y) \in R[[x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n]]$$

satisfying the conditions above.

It is known that if R is torsion free, there are power series

$$f_i(x) \in R \otimes \mathbf{Q}[[x_1, x_2, \ldots, x_n]]$$

(called the *logarithm of* F) such that

$$F(x, y) = f^{-1}(f(x) + f(y)).$$

Here is an example that motivates this terminology. For $n = 1$, let

$$F(x, y) = x + y - xy = 1 - (1 - x)(1 - y),$$

the multiplicative formal group law. Then by a well known calculus exercise,

$$f(F(x, y)) = f(x) + f(y),$$

where

$$f(x) = \sum_{i=1}^{\infty} \frac{x^i}{i},$$

the power series expansion for the natural logarithm of $1/(1 - x)$. Note that f is a power series over $\mathbf{Q}$, but F is defined over $\mathbf{Z}$.

More generally, any vector $f(x)$ of power series over $R \otimes \mathbf{Q}$ satisfying

$$f(x) \equiv x \qquad \mod (x)^2$$

leads to a formal group law

$$F(x, y) = f^{-1}(f(x) + f(y))$$

defined over $R \otimes \mathbf{Q}$. *The subtlety of the theory is finding conditions on f that guarantee that F is defined over R.* In most cases $f(x)$ can be written explicitly but $F(x, y)$ cannot.

3. Dieudonné's examples $G_{m,n}$

Now we will describe some interesting examples of higher dimensional commutative formal group laws over $\mathbf{Z}_{(p)}$ for a prime p. Let m and n be nonnegative integers with $m > 0$, and $\gcd(m, n) = 1$. Then $G_{m,n}$ is the m-dimensional formal group law with logarithm given by

$$f_k = \sum_{i \geq 0} \frac{x_{k+i}^{p^i}}{p^i} \qquad \text{for } 1 \leq k \leq m,$$

where $x_j = x_{j-m}^{p^n}$ for $j > m$. In particular, $G_{1,n-1}$ for $n > 0$ is the 1-dimensional formal group law with

$$f(x) = \sum_{i \geq 0} \frac{x^{p^{ni}}}{p^i}.$$

The integrality of $G_{m,n}$ is far from obvious. One can also define $G_{0,1}$ (an étale group) in a similar way, but that is another story.

The following facts are known about the $G_{m,n}$.

- Let $\overline{G}_{m,n}$ denote the mod p reduction of $G_{m,n}$. Over the algebraic closure of $\mathbf{F}_p$, any formal group law is isogenous to a direct sum of $\overline{G}_{m,n}$s.
- If we define $\overline{G}_{jm,jn}$ as above for $j > 1$ (so that the two indices are not relatively prime), then it is isogenous to the direct sum of j copies of $\overline{G}_{m,n}$.
- As a Hopf algebra, $\overline{G}_{m,n}$ is dual to $\overline{G}_{n,m}$. In particular, $\overline{G}_{1,1}$ is self-dual.
- If the formal group law associated with an abelian variety in characteristic p has a summand isogenous to $\overline{G}_{m,n}$, then it also has one isogenous to $\overline{G}_{n,m}$. This is called the *Riemann symmetry condition.*
- The formal group law associated with an elliptic curve in characteristic p is isogenous to either $\overline{G}_{1,0}$, the ordinary case, or $\overline{G}_{1,1}$, the supersingular case.

4. Some algebraic curves

An algebraic curve of genus g defined over a ring R has associated with it a g-dimensional formal group law, the formal completion of its Jacobian. If the curve has good mod p reduction, we get a formal group law in characteristic p, which we can try to describe in terms of the $\overline{G}_{m,n}$ above.

We will state two theorems in this direction, one for the Fermat curve defined by

$$x^d + y^d = 1$$

where the degree d is not divisible by p, and for the Artin-Schreier curve defined by

$$y^e = x^p - x$$

for e not divisible by p.

These are originally due to Honda and Manin respectively. Manin's proof for the Artin-Schreier curve (which was outlined in papers of Katz and Koblitz) was quite sophisticated and used information about the zeta function of the curve.

Honda's proof for the Fermat curve was more direct and his methods are more widely applicable. In particular, we have applied them to the Artin-Schreier curve.

Both methods require some subtle p-adic analysis, and both theorems can be stated in simple combinatorial terms.

The Fermat curve of degree d

Recall that p is a prime not dividing d. Let h denote the multiplicative order of p modulo d, i.e., the smallest positive integer for which $p^h - 1$ is divisible by d.

Let

$$\begin{aligned} M &= \{(i,j)\colon 0 < i, j < d,\, i \neq j\} \\ M_0 &= \{(i,j)\colon 0 < j < i < d,\} \end{aligned}$$

The genus of the curve is $\binom{d-1}{2}$, the cardinality of M_0, which is half the cardinality of M.

Multiplication by p modulo d acts on the set M, decomposing it into S orbits $M(s)$ for $1 \leq s \leq S$, each having cardinality dividing h. Let

$$M_0(s) = M(s) \cap M_0$$

and suppose that it has $m(s)$ elements. Let $n(s)$ denote the number of remaining elements in $M(s)$. Then Honda shows that the formal group law for the Jacobian decomposes into S summands with the sth summand corresponding to a copy of the $\overline{G}_{m(s),n(s)}$ over the algebraic closure of $\mathbf{F}_p$. Note that if the orbit of (i,j) yields a copy of $G_{m,n}$, then that of (j,i) will give $G_{n,m}$, so the Riemann symmetry condition is satisfied.

For example, let $(p,d) = (3,5)$, for which $h = 4$ and the genus is 6. Then the action on M is given by

$$\begin{array}{ccccccccc} (1,2) & \to & (3,1) & \to & (4,3) & \to & (2,4) & \to & (1,2) \\ (1,3) & \to & (3,4) & \to & (4,2) & \to & (2,1) & \to & (1,3) \\ (1,4) & \to & (3,2) & \to & (4,1) & \to & (2,3) & \to & (1,4) \end{array}$$

Hence there are three orbits each having 4 elements, 2 of which lie in M_0. Thus we get 3 copies of $G_{2,2}$, which is isogenous to 6 copies of $G_{1,1}$.

For $p = 3$, the only values of d with $h = 4$ are the divisors of 80 which are not divisors of 8. [More generally for given p and h, d must be a divisor of $p^h - 1$ which is not a divisor of $p^{h'} - 1$ for any $h'|h$.] There are no $G_{1,3}$ factors for d dividing 10; 12 such factors for $d = 16$ and $d = 20$; 84 for $d = 40$ and 324 for $d = 80$.

The Artin-Schreier curve of degree e

Now we consider the curve defined by

$$y^e = x^p - x$$

where p does not divide e. Experience has shown that the most interesting case is $e = p^f - 1$ for a positive integer f. The genus of this curve is

$$g = (e-1)(p-1)/2.$$

It is known to be covered by the Fermat curve of degree $d = (p-1)e$.

As before, let h denote the multiplicative order of p modulo d (when $e = p^f - 1$, $h = (p-1)f$), and let

$$\begin{aligned} M &= \{ei + j \colon 0 \le i < p-1,\ 0 < j < e\} \\ &= \{k \colon 0 < k < d,\ e \nmid k\} \\ M_0 &= \{ei + j \in M \colon ei + pj < d\} \end{aligned}$$

As before, the genus is the cardinality of M_0, which is half that of M.

Multiplication by p modulo d acts on the set M, decomposing it into S orbits $M(s)$ for $1 \le s \le S$, each having cardinality dividing h. The formal group law has description similar to that in the Fermat case. The Riemann symmetry condition follows from the fact that for each $k \in M$, exactly one element of $\{k,\ d-k\}$ is in M_0, so the orbits of k and $d-k$ yield dual factors.

For example, when $e = p^{f-1}$ and $(p, f) = (3, 2)$, we have $g = 7$, $d = 16$, $h = 4$, and

$$\begin{aligned} M &= \{k\colon 0 < k < 16,\ 8 \nmid k\} \\ M_0 &= \{1,\ 2,\ 3,\ 4,\ 5,\ 9,\ 10\} \end{aligned}$$

The orbit of 5 is $\{5,\ 15,\ 13,\ 7\}$, which yields a factor isomorphic to $G_{1,3}$, a 1-dimensional formal group law of height 4.

More generally, the orbit of the integer

$$\ell = (m-1)/p = p^f - p^{f-1} - 1$$

yields a unique factor isomorphic to $G_{1,h-1}$, a 1-dimensional formal group law of height h.

University of Rochester, Rochester, NY 14627