GENERALIZING THE BERNOULLI NUMBERS
UNDERGRADUATE RESEARCH PROJECT WITH MIESZKO KOMISARCZYK AND PAWEL POCZOBUT

IM PAN

JUNE 13 – 18, 2016

MASHA VLASENKO

The classical Bernoulli numbers

$$B_0 \;=\; 1\,,\; B_1 \;=\; -\frac{1}{2}\,,\; B_2 \;=\; \frac{1}{6}\,,\; B_3 \;=\; 0\,,\; B_4 \;=\; -\frac{1}{30}\,,\;\dots$$

can be defined as the coefficients in the power series expansion

$$\frac{x}{e^x-1} \;=\; \sum_{n=0}^{\infty} B_n\,\frac{x^n}{n!}\,.$$

This sequence of numbers shows up in several deep results in diverse branches of mathematics, including mathematical physics, algebraic topology and number theory. Please have a quick look at the article "Bernoulli numbers and the unity of mathematics" by Barry Mazur (it can be easily found on the web).

We shall consider the following generalization of the Bernoulli numbers. A *formal group law* (of dimension 1, over $\mathbb{Z}$) is a formal power series in two variables

$$F(x,y) \;=\; \sum_{i,j=0}^{\infty} a_{ij}\,x^i y^j\,, \quad a_{ij}\in\mathbb{Z}$$

satisfying the following conditions:

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

Simple examples: $F(x,y) = x+y$ (called the *additive* formal group law); $F(x,y)=x+y+xy$ (called the *multiplicative* formal group law). The only polynomial formal group laws are $F_c(x,y)=x+y+cxy$ with a parameter $c\in\mathbb{Z}$.

Surprisingly, conditions (i) and (ii) imply that $F(x,y)=F(y,x)$ (i.e. our formal group law is automatically *commutative*) and there exists a unique formal power series of the form

$$f(x) = x + \sum_{i=2}^{\infty} b_i x^i\,, \quad b_i\in\mathbb{Q}$$

such that $F(x,y)=f^{-1}(f(x)+f(y))$. Here $f^{-1}(x)$ is the formal inverse series, that is a unique formal series

$$f^{-1}(x) = x + \sum_{i=2}^{\infty} c_i x^i\,, \quad c_i\in\mathbb{Q}$$

satisfying $f^{-1}(f(x)) \;=\; x$. (You could check that such a series exists and satisfies $f(f^{-1}(x))=x$.) The above power series $f(x)$ and its formal inverse $f^{-1}(x)$ are called the *logarithm* and the *exponent* of $F(x,y)$ and denoted

$$\log_F(x) := f(x) \qquad \exp_F(x) := f^{-1}(x)$$

respectively.

The *generalized Bernoulli numbers* $\{B_n^F; n\geq 0\}$ attached to a formal group law $F(x,y)$ are defined from the expansion

$$\frac{x}{\exp_F(x)} \;=\; \sum_{n=0}^{\infty} B_n^F\,\frac{x^n}{n!}\,.$$

Exercises:

- Check that the classical Bernoulli numbers correspond to $F(x,y)=x+y+xy$.

- Check that
$$F(x,y) \;=\; x\sqrt{1-4y^2}+y\sqrt{1-4x^2} \;=\; x \,+\, y \,-\, 2xy^2 \,-\, 2yx^2 \,-\, \dots$$
is a formal group law. Compute several beginning terms of the respective Bernoulli sequence. Write down the generating series for $\{B_n^F; n\ge 0\}$.

In the course of this project we will try to generalize various properties of the classical Bernoulli numbers to the sequences $\{B_n^F; n \ge 0\}$.
For our first meeting:

- Create a list of properties of the classical Bernoulli numbers and be ready to show their proofs.
- Experiment whether the numbers $\{B_n^F; n\ge 0\}$ from the above exercise have those properties.
- Try to read through Chapters I and II of the book "p-adic numbers, p-adic analysis and zeta functions" by Neal Koblitz.

I am particularly interested in generalizing the p-adic properties of the classical Bernoulli numbers. By this I mean the following two facts. The *Clausen – von Staudt theorem* tells us which primes occur in the denominator of B_n:
$$B_n + \sum_{p:(p-1)|n} \frac{1}{p} \in \mathbb{Z}\,.$$
The *Kummer congruence* tells us that
$$\frac{B_n}{n} \equiv \frac{B_m}{m} \mod p \quad \text{whenever} \quad n \equiv m \not\equiv 0 \mod (p-1)$$
and, more generally, for $k \ge 0$ one has
$$(1-p^{n-1})\,\frac{B_n}{n} \equiv (1-p^{m-1})\,\frac{B_m}{m} \mod p^{k+1} \quad \text{whenever} \quad n\equiv m \mod p^k(p-1)\,,\quad n,m \not\equiv 0 \mod (p-1)\,.$$
Generalization of the Kummer congruence for $\{B_n^F; n\ge 0\}$ is an open research question. Chapter I of the book by Neal Koblitz will introduce you to p-adic analysis. In Chapter II you will find insights into the above mentioned p-adic properties of the classical Bernoulli numbers.

Some research questions

1. *Computing "special values" from Kummer's congruences*

   Here we will deal with the classical Bernoulli numbers. Pick an even integer $1 \le a \le p-2$ consider the set of natural numbers
$$U_a = \{n \in \mathbb{N} : n \equiv a \mod p-1\}\,.$$
   By Kummer's theorem, the function
$$\mathcal{K}(n) \;=\; (1-p^{n-1})\,\frac{B_n}{n}$$
   is p-adically continuous on U_a. Since U_a is dense in $\mathbb{Z}_p$, we can extend $\mathcal{B}$ to a unique p-adically continuous function $\mathcal{K}_a : \mathbb{Z}_p \to \mathbb{Z}_p$. Try to compute the values of $\mathcal{K}_a(x)$ at various points of $\mathbb{Z}_p \setminus U_a$, e.g. $x = 0, -1, \frac{1}{2}, \dots$
2. *Sums of powers of consecutive integers via formal group laws*

   In the classical case Bernoulli polynomials are defined by the generating function
$$\frac{x\,e^{tx}}{e^x-1} \;=\; \sum_{n=0}^{\infty} B_n(t)\frac{x^n}{n!}\,.$$
   Try to define Bernoulli polynomials for a formal group law in such a way that would also give a natural generalization of the formula
$$\sum_{i=1}^{m} i^n \;=\; \frac{B_{n+1}(m) - B_{n+1}(0)}{n+1}\,.$$
   In particular, explain how the left-hand side here is related to the multiplicative formal group law $F(x,y) = x+y+xy$ which produces the classical Bernoulli numbers.

3. *Generalizing Kummer's congruence*

Let $F(x,y) \in \mathbb{Z}[\![x,y]\!]$ be a formal group law. Our ultimate goal is to generalize Kummer's congruence for the sequence $\{B_n^F; n \geq 0\}$. For this we need to guess the function which will be p-adically continuous, like $\mathcal{K}(n)$ in the classical case. I expect that for each p the correction factor, say an analogue of $(1-p^{n-1})$, should depend on the characteristic polynomial of the reduction of the formal group law $F(x,y)$ modulo p. (See the section on formal group laws over finite fields.) When the height at p is 1 then the characteristic polynomial is $P(T) = p - u_p T$ for some p-adic unit $u_p \in \mathbb{Z}_p^\times$, and I propose the following

Conjecture. *The function*

$$\mathcal{K}^F(n) \;=\; u_p^{\lfloor \frac{n}{p-1} \rfloor}\,(1-p^{n-1})\,\frac{B_n^F}{n}$$

is p-adically continuous on the set $U_a = \{n \in \mathbb{N} : n \equiv a \mod p-1\}$ for every $1 \leq a \leq p-2$. Namely, if $n, m \in U_a$ and $n \equiv m \mod p^k$ then $\mathcal{K}^F(n) \equiv \mathcal{K}^F(m) \mod p^{k+1}$.

We could approach this conjecture by working with particular of formal group laws. The simplest example might be our "circular" law $F(x,y) = x\sqrt{1-4y^2} + y\sqrt{1-4x^2}$. Here for each $p \neq 2$ the height is 1 and $u_p = (-1)^{\frac{p-1}{2}}$ (try to prove it yourself). Next, one could try "elliptic" formal group laws (we describe them in a separate section at the end).

Some ideas to attack the problem:

- Try to generalize the proof of Kummer's congruence in Lang's book "Introduction to modular forms" using the generating function: (1) to higher powers of p; (2) to other formal groups. (Mind that the Kummer congruence modulo p is known in general, see the section on the universal approach below.)
- Try to generalize the p-adic measures in Chapter II of Koblitz's book to other formal groups.

Universal approach to generalized Bernoulli numbers

Consider the formal power series

$$f(x) \;=\; x + b_1\,\frac{x^2}{2} + b_2\,\frac{x^3}{3} + \ldots \;=\; \sum_{n=1}^{\infty} b_{n-1}\frac{x^n}{n}\,, \qquad b_0 \;=\; 1\,,$$

where $b_1, b_2, \ldots$ are variables. Form the inverse power series

$$f^{-1}(x) \;=\; x - b_1\,\frac{x^2}{2} + (3\,b_1^2 - 2\,b_2)\,\frac{x^3}{6} - \ldots$$

and consider the *universal formal group law* $F(x,y) \;=\; f^{-1}(f(x)+f(y))$ along with the *universal Bernoulli "numbers"* $\widehat{B}_n \in \mathbb{Q}[b_1, b_2, b_3, \ldots]$. Study basic properties of the polynomials $\widehat{B}_n$. For example:

- Assign weights to the variables $b_1, b_2, \ldots$ so that each monomial in $\widehat{B}_n$ has weight n.
- Let d_n be the least common multiple of the denominators of the coefficients of $\widehat{B}_n$. What can be proved about the sequence $\{d_n; n \geq 1\}$?

Answers to the above questions can be found in the literature listed below. The Clausen – von Staudt theorem was generalized to the universal case by Clarke ([2, Corollary 6]):

$$\widehat{B}_n + \sum_{\substack{p \text{ prime} \\ p-1|n}} \frac{1}{p}\, b_{p-1}^{\frac{n}{p-1}} \;\in\; \mathbb{Z}[b_1, b_2, \ldots]\,.$$

Adelberg ([3, Theorem 3.2]) proved Kummer's congruence modulo p:

$$\frac{\widehat{B}_{n+p-1}}{n+p-1} \equiv b_{p-1}\,\frac{\widehat{B}_n}{n} \mod p\,\mathbb{Z}[b_1, b_2, \ldots]$$

for any $n \not\equiv 0, 1 \mod p-1$. (There is a corrected version for $n \equiv 1 \mod p-1$.)

In [4] Adelberg tried to improve his universal congruence modulo prime powers. However his approach is weaker than we would like to because of the present bound on s below. By [4, Theorem 4.5] when $n \neq 0, 1$ mod $(p-1)$ one has

$$\frac{\widehat{B}_{n+kp^s(p-1)}}{n+kp^s(p-1)} \equiv b_{p-1}^{kp^s}\,\frac{\widehat{B}_n}{n} \mod p^{s+1}\,\mathbb{Z}[b_1, b_2, \ldots]$$

for all $s \leq n-2$. (There is also a correction of the above result for the case $n \equiv 1 \mod p-1$.)

- Check that Adelberg's results agree with our conjecture. You can use the following result: by [5, Theorem 2] the height of the reduction of the formal group law $F(x,y) \in \mathbb{Z}[\![x,y]\!]$ modulo p equals 1 if and only if $p \not| b_{p-1}$. In the latter case all b_{p^k-1} are p-adic units and $u_p \equiv b_{p^k-1}/b_{p^{k-1}-1} \mod p^k$ for each $k \geq 1$. In particular, $u_p \equiv b_{p-1} \mod p$.

Homorphisms, isomorphisms and endomorphisms of formal group laws

Suppose we have a commutative ring R, two (one-dimensional) formal group laws $F, G \in R[\![x,y]\!]$ and a ring R' which contains R (it might coincide with R or be a larger ring). A *homomorphism* from F to G over R' is a formal power series $h \in R'[\![x]\!]$ such that $h(0) = 0$ and $h(F(x,y)) = G(h(x), h(y))$. A homomorphism $h(x) = c_1 x + c_2 x^2 + \dots$ is called an *isomorphism* if c_1 is a unit in R' (under this condition we have the inverse series $h^{-1}(x) = c_1^{-1} x + \ldots \in R'[\![x]\!]$) and we say that F and G are *isomorphic* over R'. If $c_1 = 1$ we call h a *strict isomorphism* and say that F and G are *strictly isomorphic* respectively.

For example, every formal group law $F \in \mathbb{Q}[\![x,y]\!]$ is strictly isomorphic to the additive formal group law $x+y$ over $\mathbb{Q}$, the strict isomorphism being given by the logarithm $h(x) = \log_F(x) = \int_0^x dy \Big/ \frac{\partial F}{\partial y}(0,y)$.

When $F \in R[\![x,y]\!]$ is commutative ($F(x,y) = F(y,x)$), one can define the following homomorphisms from F to itself (such homomorphisms are called *endomorphisms*), defined over R for $n \geq 1$:

$$[n]_F(x) \;=\; \underbrace{F(x, F(x, \dots (F(x,x)}_{n} \dots) \;=\; nx \,+\, \dots$$

They are called "multiplication by n endomorphisms". We have $[1]_F(x) = x$ (convention), $[2]_F(x) = F(x,x), [3]_F(x) = F(x, F(x,x))$ and so on.

Formal group laws over finite fields

Assume now that $F(x,y) \in \mathbb{F}_p[\![x,y]\!]$. In this case, in addition to the usual endomorphisms $[n]_F(x)$, we have the *Frobenius* endomorphism given by

$$\phi(x) \;=\; x^p\,.$$

- Check that $\phi(x)$ is an endomorphism.

The *height* of a homomorphism $h(x)$ of two formal group laws $F, G \in \mathbb{F}_p[\![x,y[\![$ is defined as the smallest $m \geq 0$ such that there exist $g(x) = c_1 x + \in \mathbb{F}_p[\![x]\!]$ with $c_1 \neq 0$ and $h(x) = g(x^{p^m})$. By convention, the height is ∞ if $h = 0$. The height is known to be well defined.

The height $ht(F)$ of a commutative formal group law $F(x,y) \in \mathbb{F}_p[\![x,y]\!]$ is by definition the height of the endomorphism $[p]_F$.

- Explain why $ht(F) \geq 1$.
- For the multiplicative law $F(x,y) = x + y + xy$ over $\mathbb{Z}$ compute the endomorphisms $[n]_F$ and the height at each p.

Theorem.([1]) *Let $F(x,y) \in \mathbb{F}_p[\![x,y]\!]$ be a commutative formal group law. If $ht(F) = \infty$ then F is isomorphic to $x+y$ over $\mathbb{F}_p$. Assume $h = ht(F) < \infty$. Then there exist p-adic numbers $\alpha_1, \dots, \alpha_{h-1} \in p\mathbb{Z}_p$ and $\alpha_h \in \mathbb{Z}_p^\times$ such that the Frobenius endomorphism ϕ satisfies the equation*

$$p + \sum_{i=1}^{h} \alpha_i \phi^i \;=\; 0.$$

The polynomial $P(T) \;=\; p + \sum_{i=1}^h \alpha_i T^i$ is called the *characteristic polynomial* of F. It is an irreducible polynomial (by Eisenstein's criterion). If $ht(F) = \infty$ we put $P(T) = p$ by convention.

- Compute the characteristic polynomial of the multiplicative law $F(x,y) = x + y + xy$ at each p.
- Compute the characteristic polynomial of the circular group law $F(x,y) = x\sqrt{1-4y^2} + y\sqrt{1-4x^2}$ at each p.

Theorem.([1]) *Two formal group laws over $\mathbb{F}_p$ are isomorphic if and only if their characteristic polynomials are equal.*

Elliptic formal group laws

Consider the formal series $f(x) = \sum_{n=1}^{\infty} b_{n-1}x^n/n$ where $b_0 = 0$ and $b_n \in \mathbb{Z}[a, b]$ are defined as

$$b_n = \begin{cases} \text{the coefficient of } u^{n-1} \text{ in } (u^3 + au + b)^{(n-1)/2}\,, & n \text{ odd,} \\ 0\,, & n \text{ even.} \end{cases}$$

As usual, we define the formal group law $F(x, y) = f^{-1}(f(x) + f(y))$.

- Show that the coefficients of $F(x, y)$ belong to $\mathbb{Z}[a, b]$. (This might be a very difficult question, you can read further without doing it.)

We will work with this formal group law in the case when $a, b \in \mathbb{Z}$ are integers such that the polynomial $u^3 + au + b$ has no multiple roots.

Remark (on algebraic geometry): *In this case the above formal group law $F(x, y)$ arises from the situation discussed by us during the week: there is an algebraic curve (call it $E = E_{a,b}$) with a group law and a fixed parametrization around the point which represents the unit in the group. This curve is given by the equation*

$$E\;:\;v^2 \;=\; u^3 + au + b\,.$$

Such curves are called elliptic curves*, and we could have taken any cubic polynomial (say, with real coefficients) in the right-hand side. If this cubic polynomial has no multiple roots, then the curve is smooth and one can turn it into an abelian group. However the story becomes a bit tricky at this stage: one has to extend the picture from the usual plane $\mathbb{R}^2$ to the projective plane $\mathbb{P}^2(\mathbb{R})$, there our curve will get exactly one extra point (call this point $\mathcal{O}$ and let $\overline{E} = E \cup \mathcal{O}$ be the projectivization of E). This extra point $\mathcal{O}$ "at infinity" is the unit element in the group law on the curve. Please ask Piotr how to turn an elliptic curve into a group, this construction is very interesting! Moreover: $t = -u/v$ can be taken as a parameter around the point $\mathcal{O}$ at infinity; the differential du/v is invariant under the group law, and its expansion with respect to t is given by*

$$\frac{1}{2}\frac{du}{v} \;=\; \frac{1}{2}\frac{u'(t)}{v(t)}dt \;=\; \Big(1 + 2a\,t^4 + 3b\,t^6 + 6a^2\,t^8 + 20ab\,t^{10} + \ldots\Big)dt \;=\; \Big(\sum_{m=0}^{\infty} b_m t^m\Big)dt$$

with the coefficients b_m defined above. I don't expect you understand the precise meaning of these words. You can skip the remark or ask Piotr to explain more.

For each prime p consider the integer number

$$a_p \;=\; p \,-\, \#E(\mathbb{F}_p) \;=\; p \,-\, \#\{(u, v) \in \mathbb{F}_p^2 : v^2 = u^3 + au + b\}\,.$$

Remark. *This number is related to the local zeta function of the elliptic curve E as follows. Assume that the polynomial $u^3 + au + b \mod p$ has no multiple roots. (To be precise: p doesn't divide the discriminant of $u^3 + au + b$, which is given by $\Delta = 4a^3 + 27b^2$.) In this case E gives a smooth curve over $\mathbb{F}_p$ is the sense of algebraic geometry and the zeta function of its projectivization $\overline{E} = E \cup \mathcal{O}$ is given by $Z(\overline{E}/\mathbb{F}_p; T) = \frac{1-a_pT+pT^2}{(1-T)(1-pT)}$.* You don't have to prove this fact, it requires techniques we didn't discuss. However you could check it for particular curves on a computer.

Assume that $p \not|\Delta$ and $p \not|a_p$. In this case the height of the reduction of $F(x, y)$ modulo p is 1 and the characteristic polynomial is equal to $P(T) = p - u_pT$ where $u_p \in \mathbb{Z}_p^\times$ is the unique p-adic unit solution to $u^2 - a_pu + p = 0$. (Again, this fact requires techniques we didn't discuss, don't try to prove it.) If you wish to try our conjecture in this case, note that $u_p \equiv a_p \mod p$.

References

[1] M. Hazewinkel, *Formal group laws*, 1978

[2] F. Clarke, *The universal von Staudt theorems*, Transactions of AMS vol. 15, no. 2 (1989) pp. 591–603

[3] A. Adelberg, *Universal Higher Order Bernoulli Numbers and Kummer and Related Congruences*, Journal of Number Theory 84 (2000), pp.119–135

[4] A. Adelberg, *Universal Kummer congruences mod prime powers*, Journal of Number Theory 109 (2004), pp.362–378

[5] M. Vlasenko, *Formal groups and congruences*, http://arxiv.org/abs/1509.06002