Corrections to my article *How can we construct abelian Galois extensions of basic number fields?* and comments.

B. Mazur

June 16, 2011

My article appeared in the Bulletin of that American Mathematical Society: Bull. Amer. Math. Soc. **48** (2011), 155-209.

1 The 200-th Bernoulli number

In footnote 20 on page 168 I claimed that the numerator of the fraction $-B_{200}/400$, where B_{200} is the two-hundredth Bernoulli number has the following decomposition

$$389 \cdot 691 \cdot 5370056528687 \quad \text{times this } 204-\text{digit number :}$$

$N :=$ 345269032939215803146410928173696740406844815684239672101299206421451944591925694154456527606766236010874972724155570842527652727868776362959519620872735612200601036506871681124610986596878180738901486527

and I *incorrectly asserted* that that last factor N is a prime number.

I am grateful to Bartosz Naskręçki who spotted this error: our 204-digit factor N above is *not* prime because it fails the *Fermat 2-test*! (I.e., 2^N is not 2 mod N.) Naskręçki wrote that he ran SAGE programs (attempting a factorization of N) on his laptop and on a big 16-core machine for 24 hours but no factor was found.

Extensive data on factorization of Bernoulli numbers is on the web-site

http://homes.cerias.purdue.edu/ ssw/bernoulli/index.html

constructed by Samuel Wagstaff. At the very bottom of the chart there one finds a list of composite numbers whose factorizations have resisted all factorization attempts to date; B_{200} is 12th on the list:

http://homes.cerias.purdue.edu/ ssw/bernoulli/composite.

I consulted William Stein about this number N and he responded:

> That number has 677 bits, so it *could* be factored using techniques that exist. If you look at http://en.wikipedia.org/wiki/Integer_factorization you'll get a sense of who and what does this sort of thing (e.g., "required several months of computer time using the combined power of 80 AMD Opteron CPUs."). However, general purpose programs like Sage/Magma can't touch this. That is, unless you got really lucky and that 677 bit number were a product of a number with < 20 digits say, which Lenstra's elliptic curve method could pick off...

I consulted Samuel Wagstaff about N and he responded:

> I am writing a book about applications of factoring and will refer to your paper in the section on applications of factoring Bernoulli numerators.
>
> The Bernoulli factors web-page is up-to-date. Therefore, no factor is known for the 204-digit composite N you list below.
>
> The record for factoring by the general number field sieve is about 192 digits. No other algorithm could certainly factor a hard 204-digit composite. The best one could do is try the elliptic curve method and hope N has a factor with no more than about 60 or 65 digits. I will do this over the next few weeks and let you know if a factor of N is found. From earlier work on numbers in the table, I am pretty sure that N has no prime factor smaller than 50 digits.

2 Further (and up-dated) references

1. Jean-Pierre Serre informed me of a reference to a version of "Ribet's Lemma" (but only for representations of *finite* groups G) that was in print even before Ribet's article. This is an article by John Thompson:

   J.G.Thompson, "Vertices and Sources" , J.Algebra **6** (1967), pp.1-6 (cor.au th.1).

2. Eric Urban informed me that Reference 66 in my paper, which is to a url for the forthcoming article by Skinner and Urban, is available by going to a (slightly) changed url: http://www.math.columbia.edu/ urban/EURP.html

3 Misstatements, Awkward statements, Mathematical Typos etc.

I am thankful to Khoa Nguyen, Chandan Dalawat, and Marius Stefan for close readings of my article and for providing me with elements in this list of corrections.

1. Footnote 15 (page 165) has a phrase missing; it should read: "If this happens, then "enough" of the fundamental theorem of arithmetic holds in the ring of integers of $\mathbb{Q}(e^{2\pi i/p})$ to allow one to prove Fermat's Last Theorem for the exponent p; it will not work for the exponent 691."

2. Page 166, Footnote 16, Line ?8, replace unramfied by unramified.

3. Page 178, Theorem 4, Line 6, replace t_ℓ by $t(\ell)$.

4. Page 178, Theorem 4, Line 6, replace O in $\emptyset_\lambda$ by O_λ.

5. Page 179 line 4 and footnote 33: I wrote $f_{w_0} = f$ and $f = f_{w_0}$ respectively; but that's not correct if f is a (p-ordinary) newform of weight $k \geq 2$ on $\Gamma_0(N)$ *when N is prime to p*: in that case we need to bring f to $\Gamma_0(N) \cap \Gamma_1(p)$ (in the following standard way). We view such a form f as having Fourier coefficients in the ring of integers of a specific finite discrete valuation ring and—since f is p-ordinary—its p-th Fourier coefficient a_p is a unit in this ring. Let u_p be the (unique) p-adic unit root of $X^2 - a_pX + p^{k-1}$ and define:

   $f' :=$ the p-ordinary eigenform for U_p on $\Gamma_0(N) \cap \Gamma_1(p)$ obtained from f by the formula: $f'(z) := f(z) - \frac{p^{k-1}}{u_p} f(pz)$.

   We want our formulas to read: $f_{w_0} = f'$ and $f' = f_{w_0}$ respectively This same correction holds also on page 180, line 24 where the (incorrect) parenthetic phrase: "(Indeed $\Phi_{12} = \Delta$)" should be replaced by "(Indeed $\Phi_{12} = \Delta'$)" where, again, Δ' is the p-ordinary eigenform for U_p on $\Gamma_0(N) \cap \Gamma_1(p)$ related, by the above equation, to Δ.

6. Page 183, Section 15, Line 1, replace $\kappa = \mathbf{Q}_p$ by $\mathcal{K} = \mathbf{Q}_p$.

7. Page 183, Section 15, Line 5, replace $\pi^{-m}\mathcal{O} \in \mathcal{K}$ by $\pi^{-m}\mathcal{O} \subset \mathcal{K}$.

8. The statement "Denote the kernel of the projection $M^{(0)} \otimes \kappa \to \overline{r}^{(0)}$ by $\overline{r}_1$" in Step 1 on page 185 should perhaps be replaced by " "Denote the kernel of the projection $M^{(0)} \otimes \kappa \to \overline{r}_0$ by $\overline{r}_1$".

9. In the footnote 42 on page 188, "$k[G]$" should read instead "$\kappa[G]$".

10. In the third paragraph on page 192, " "$\kappa = \mathbb{Q}_5$" should be "$\mathcal{K} = \mathbb{Q}_5$". The statement (in the same paragraph)"The two indecomposable residual representations are the representations of Galois on the 5-torsion of the two other elliptic curves over $\mathbb{Q}$ of conductor 11" should read instead: "The two indecomposable residual representations are the representations of Galois on the 5-torsion of the two elliptic curves $X_1(11)$ and $X_{-1}(11)$".

11. "Improperly irregular" in footnote 55 (page 197) should actually read "properly irregular."

12. Page 191, Corollary 6, Line 1, replace $r_{\Delta,691}$ by $\rho_{\Delta,691}$.

13. Page 191, Corollary 6, Line 4, replace $r_{w,691}$ by $\rho_{w,691}$.

14. On page 202 line 17: remove the word "'by" from the phrase: "denote the Λ-module by $\mathbb{Z}_p$, where the Λ-action is given via s_k by the symbol $\mathbb{Z}_p\langle k\rangle$"

15. Page 205, Line 21, replace "weight k" by "weight 2k".