Prime divisors of the Bernoulli and Euler numbers

Samuel S. Wagstaff, Jr.*
Center for Education and Research
in Information Assurance and Security
and Department of Computer Sciences, Purdue University
West Lafayette, IN 47907-1398 USA

Abstract

We have completely factored the numerators N_{2k} of the Bernoulli numbers for all $2k \leq 152$ and the Euler numbers E_{2k} for all $2k \leq 88$, using the even index notation. We studied the results seeking new theorems about the prime factors of these numbers. We rediscovered two nearly-forgotten congruences for the Euler numbers.

1 Factoring the Bernoulli and Euler numbers

The Bernoulli numbers B_n may be defined by the generating function

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

The B_n are all rational numbers, $B_{2k+1} = 0$ for all $k \geq 1$, and the non-zero B_n alternate in sign. The first few non-zero ones are: $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, $B_{10} = 5/66$, $B_{12} = -691/2730$, $B_{14} = 7/6$, $B_{16} = -3617/510$, $B_{18} = 43867/798$. B_{20} is the first one with a composite numerator: $174611 = 283 \cdot 617$.

Write B_n as N_n/D_n with $D_n > 0$ and $\gcd(N_n, D_n) = 1$. It is easy to describe the denominators:

* This work was supported in part by the Purdue University CERIAS and by the Lilly Endowment, Inc.

Theorem 1 (von Staudt-Clausen [34, 9] 1840) *If* $n > 0$, *then*

$$D_n = \prod_{\substack{p \text{ prime} \\ p-1|n}} p, \quad \textit{and} \quad B_n + \sum_{\substack{p \text{ prime} \\ p-1|n}} \frac{1}{p} \quad \textit{is an integer}.$$

If a prime p divides some numerator N_n, then it divides every $p-1$-st numerator after that:

Theorem 2 (Kummer [19] 1851) *If* $n \geq 1$, p *is a prime* ≥ 5 *and* $p-1 \not| 2n$, *then*

$$\frac{B_{2n+(p-1)}}{2n+(p-1)} \equiv \frac{B_{2n}}{2n} \bmod p.$$

Another useful fact about the prime factors of N_n is this:

Theorem 3 (J. C. Adams [1] 1878) *If* p *is prime,* $n \geq 1$, $p-1 \not| 2n$ *and* $p^e | 2n$ *for some* $e \geq 1$, *then* $p^e | N_{2n}$.

Slavutskii [27] attributes both Kummer's congruence and Adams' theorem to two obscure pamphlets [35] of von Staudt. See also [28]. The Bernoulli numbers and the prime factors of their numerators have been of fundamental importance in the study of cyclotomic fields since the time of Kummer. For example, see Iwasawa [16] and Ribenboim [25]. Before Wiles proved Fermat's Last Theorem, these numbers provided an important avenue of attack on that problem.

M. Ohm [22] made the first attempt to factor Bernoulli numerators in 1840. In unpublished work, J. Bertrand, J. L. Selfridge, M. C. Wunderlich, and others, factored more Bernoulli numerators. In 1978, we [36] published the factorizations through N_{60}, but there was a typo in the very last factor. Now we have factored N_{2k} for all $2k \leq 152$ and for many larger $2k \leq 300$. See Adams [1] for the unfactored N_{2k} and the D_{2k}. See Knuth and Buckholtz [18] for a simple method of computing these numbers. We used their method to compute the numbers. We publish the factors here to aid the study of cyclotomic fields.

Some other works which consider prime factors of Bernoulli numbers, mostly with large subscripts (far beyond the range of this paper), and which extend the work of [36], include [6, 4, 5] and pages 116ff of [10].

Five tables, placed at the end of this paper to preserve continuity, summarize our efforts over many years to factor the Bernoulli numerators and the Euler numbers. The complete results are available at the web address: `http://www.cerias.purdue.edu/homes/ssw/bernoulli/index.html`.

In Table 1, we give the complete factorization of N_{2k} for $60 \leq 2k \leq 132$. In the tables, Pxx and Cxx denote prime and composite numbers with xx

digits, respectively. To keep the paper short, Tables 2 and 3 show only the large (> 11 digits) prime factors. We assume that anyone using the tables can compute the numerators and discover the small factors easily. Several modern computer algebra systems, such as Maple and Mathematica, have Bernoulli and Euler numbers and polynomials as built-in functions. If a numerator is omitted, then we know no large prime factor of it. But the numerator is not omitted if the final known factor is prime. Thus the line "144 P135" in Table 2 means that N_{144} is the product of one or more small primes (in fact, 6500309593) times a 135-digit prime, not that N_{144} is prime.

The Euler numbers E_n may be defined by the generating function

$$\frac{2e^{t/2}}{e^t+1} = \sum_{n=0}^{\infty} \frac{E_n \cdot t^n}{2^n \cdot n!} = \sum_{n=0}^{\infty} \frac{E_n}{n!} \left(\frac{t}{2}\right)^n$$

or by the formula

$$\sec x = \sum_{n=0}^{\infty} (-1)^n E_{2n} \frac{x^{2n}}{(2n)!}.$$

The Euler numbers with odd subscripts vanish: $E_{2k+1} = 0$ for all $k \geq 0$. The non-zero Euler numbers are odd integers which alternate in sign. The first few non-zero Euler numbers are: $E_0 = 1$, $E_2 = -1$, $E_4 = 5$, $E_6 = -61$, $E_8 = 1385$, $E_{10} = -50521$, $E_{12} = 2702765$.

Since the Euler numbers are all integers, there is no analogue for them of the von Staudt-Clausen Theorem. Kummer's Theorem has an analogue for E_{2n}, also proved by Kummer. We state it as Theorem 4 below. Our search for an analogue to J. C. Adams' Theorem led to the work in the next section.

The prime factors of the Euler numbers determine the structure of certain cyclotomic fields. See Ernvall and Metsänkylä [12], for example.

Most of the above remarks about factoring Bernoulli numbers apply equally to Euler numbers. We [36] published the factorizations through E_{42} in 1978. Now we have factored E_{2k} for all $2k \leq 88$ and for some larger $2k \leq 200$.

In Table 4, we give the complete factorization (if known) of E_{2k} for $40 \leq 2k \leq 112$. To save space, Table 5 shows only the large ($> 10^{11}$) prime factors. We assume that anyone using the tables can compute the Euler numbers and discover the small factors easily. If an Euler number is omitted, then we know no large prime factor of it.

We found most of the factors in the five tables by trial division and the elliptic curve method [20]. The largest two of these factors found by the elliptic curve method were the P42 of E_{150} and the P40 of N_{206}. A few large composite cofactors were finished by the quadratic sieve factoring algorithm [23], including the C114 = P37·P77 of N_{206} and the C112 = P44·P69 of E_{116}. Large primes in these tables were proved prime by the methods of the Cunningham Project [3], including the elliptic curve prime proving method [2] for the large primes. The two largest prime divisors of Bernoulli numerators known to us are the P359 factor of N_{292} and the P332 divisor of N_{298}. The largest known prime divisor of an Euler number is the P278 of E_{194}. No doubt one could easily find larger prime divisors of the Bernoulli and Euler numbers by extending the tables a little. The first incomplete factorizations in the tables are the C123 of N_{154} and the C119 of E_{90}. The elliptic curve method, using several hundred curves with a first phase limit $2 \cdot 10^6$, has been tried on these numbers and on all the other composites in the tables.

2 Congruences for the Euler numbers

In this section we prove Kummer's Theorem for Euler numbers and two little-known congruences for Euler numbers which we rediscovered by examining (the full version of) Tables 4 and 5 in search of an analogue for J. C. Adams' Theorem. We also make some historical remarks about these theorems.

The Euler polynomials may be defined by the generating function

$$\frac{2e^{xt}}{e^t+1} = \sum_{n=0}^{\infty} E_n(x)\frac{t^n}{n!}.$$

It is easy to see that $E_n = 2^n E_n(1/2)$, for $n \geq 0$, and that $E_n'(x) = nE_{n-1}(x)$, for $n > 0$. These two facts lead easily to the Taylor expansion of $E_n(x)$ about $x = 1/2$:

$$E_n(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{E_k}{2^k} \left(x - \frac{1}{2}\right)^{n-k}, \tag{1}$$

which holds for all nonnegative integers n and all real x, and which was proved by Raabe [24] in 1851.

Euler, on page 499 of [14], introduced Euler polynomials to evaluate the alternating sum

$$A_n(m) = \sum_{k=1}^{m} (-1)^{m-k} k^n = m^n - (m-1)^n + \cdots + (-1)^{m-1}1^n,$$

where m and n are nonnegative integers. The identity $E_n(x+1) + E_n(x) = 2x^n$ follows easily from the definition of Euler polynomials. Alternately adding and subtracting this identity with $x = m-1$, $x = m-2$, $\ldots$, $x = 1$, gives the formula

$$A_n(m) = \frac{1}{2}(E_n(m+1) - (-1)^m E_n(1)) \tag{2}$$

for integers m, $n \geq 0$. In the same way, one can prove that

$$C_n(b,m) \stackrel{\text{def}}{=} \sum_{k=1}^{m}(-1)^{m-k}(k+b-1)^n = \frac{1}{2}(E_n(b+m) - (-1)^m E_n(b)) \tag{3}$$

for any real b and integers m, $n \geq 0$. Setting $x = 0$ in $E_n(x+1) + E_n(x) = 2x^n$ shows that $E_n(1) = -E_n(0)$.

Lemma 1 *If n is an even positive integer, then $E_n(0) = E_n(1) = 0$.*

Proof: Substituting $x = 0$ and $x = 1$ in (1) and using the fact that $E_{2j+1} = 0$, one finds that

$$E_n(0) = 2^{-n}(-1)^n \sum_{k=0}^{n}(-1)^k \binom{n}{k} E_k = 2^{-n} \sum_{k=0}^{n} \binom{n}{k} E_k = E_n(1).$$

But we just saw that $E_n(1) = -E_n(0)$, so $E_n(1) = E_n(0) = 0$.

Proposition 1 *If $p > 0$ is odd and $n > 0$ is even, then*

$$A_n\left(\frac{p-1}{2}\right) = 2^{-n-1} \sum_{k=0}^{n} \binom{n}{k} E_k p^{n-k}.$$

Proof: Let $x = (p+1)/2$ in (1). One gets

$$E_n\left(\frac{p+1}{2}\right) = \sum_{k=0}^{n} \binom{n}{k} \frac{E_k}{2^k} \left(\frac{p}{2}\right)^{n-k} = 2^{-n} \sum_{k=0}^{n} \binom{n}{k} E_k p^{n-k}. \tag{4}$$

Let $m = (p-1)/2$ in (2). Thus, $m+1 = (p+1)/2$ and

$$A_n\left(\frac{p-1}{2}\right) = \frac{1}{2}\left(E_n\left(\frac{p+1}{2}\right) - (-1)^{(p-1)/2} E_n(1)\right).$$

The proposition now follows from (4) and Lemma 1.

Wells Johnson [17] began with a formula analogous to the one in Proposition 1 and gave p-adic proofs of many facts about Bernoulli numbers, including Theorems 1, 2 and 3. We will use similar methods to prove facts about Euler numbers.

Let e_p denote the exponential p-adic valuation on the integers or rational numbers. Thus $e_p(n) = r$ means $p^r \| n$. We will need Johnson's lemma, which follows easily from the well-known fact that $(p-1)e_p(j!) = j - \sum_{i \geq 0} d_i$, where $j = \sum_{i \geq 0} d_i p^i$ and $0 \leq d_i < p$.

Lemma 2 (Johnson [17] 1975) *If p is prime and $j \geq 1$, then*

$$e_p\left(\frac{p^j}{j!}\right) > \frac{p-2}{p-1}j.$$

We begin with the analogue of Kummer's Theorem mentioned above:

Theorem 4 (Kummer [19] 1851) *If $n \geq 1$ and $p \geq 3$ is prime, then $E_{2n+(p-1)} \equiv E_{2n} \bmod p$.*

Proof: Write $m = (p-1)/2$. Taken modulo p, the formula of Proposition 1 is

$$A_{2n}(m) \equiv 2^{-2n-1}E_{2n} \bmod p.$$

Therefore,

$$E_{2n} \equiv 2^{2n+1}\sum_{k=1}^{m}(-1)^{m-k}k^{2n} \bmod p$$

and

$$E_{2n+(p-1)} \equiv 2^{2n+(p-1)+1}\sum_{k=1}^{m}(-1)^{m-k}k^{2n+(p-1)} \bmod p.$$

But $k^{2n+(p-1)} \equiv k^{2n} \bmod p$ for $1 \leq k < p$ by Fermat's Little Theorem, and Kummer's congruence follows.

Carlitz and Levine [8] have also investigated Kummer's congruence for Euler numbers.

Here is the analogue of J. C. Adams' Theorem:

Theorem 5 *Let p be an odd prime, n a positive integer and e a nonnegative integer. Suppose $(p-1)p^e$ divides n. Then $E_n \equiv 0$ or $2 \bmod p^{e+1}$ according as $p \equiv 1$ or $3 \bmod 4$.*

Proof: Write $m = (p-1)/2$. By hypothesis, $\phi(p^{e+1}) = (p-1)p^e$ divides n. The numbers k between 1 and m are relatively prime to p, so $k^n \equiv 1 \bmod p^{e+1}$ by Euler's Theorem. Thus,

$$A_n(m) = \sum_{k=1}^{m}(-1)^{m-k}k^n \equiv \sum_{k=1}^{m}(-1)^{m-k} \bmod p^{e+1}.$$

The sum is 0 if m is even, that is, if $p \equiv 1 \bmod 4$, and 1 if m is odd, that is, if $p \equiv 3 \bmod 4$. Now $2^{-n} \equiv 1 \bmod p^{e+1}$ by Euler's Theorem, so Proposition 1 gives us

$$E_n + \sum_{k=0}^{n-1}\binom{n}{k}E_k p^{n-k} \equiv 0 \text{ or } 2 \bmod p^{e+1}$$

according as $p \equiv 1$ or $3 \bmod 4$.

To prove the theorem, it suffices to show that every term $\binom{n}{k} E_k p^{n-k}$, for $0 \le k \le n-1$, is divisible by p^{e+1}. Write $j = n-k$, so that $1 \le j \le n$. Then

$$e_p\left(\binom{n}{k} E_k p^{n-k}\right) \ge e_p\left(\binom{n}{k} p^{n-k}\right) \ge e_p(n) + e_p\left(\frac{p^j}{j!}\right).$$

By hypothesis, $e_p(n) \ge e$. By Lemma 2, $e_p(p^j/j!) > j(p-2)/(p-1)$. Now $j \ge 1$. The fraction $(p-2)/(p-1)$ is minimized (over odd primes p) when $p = 3$. Thus $e_p(\binom{n}{k} E_k p^{n-k}) > e + 1(3-2)/(3-1)$ or $e_p(\binom{n}{k} E_k p^{n-k}) \ge e+1$, which completes the proof.

Theorem 5 shows, for example, that $E_{2k} \equiv 2 \bmod 3$, $E_{4k} \equiv 0 \bmod 5$, $E_{6k} \equiv 2 \bmod 7$, $E_{6k} \equiv 2 \bmod 9$ and $E_{10k} \equiv 2 \bmod 11$ for all $k > 0$.

Carlitz [7] gave a proof very similar to the one above.

Now define

$$D_n(m) = \sum_{k=1}^{m} (-1)^{m-k}(2k-1)^n = (2m-1)^n - (2m-3)^n + \cdots + (-1)^{m-1}1^n$$

for integers $m \ge 1$, $n \ge 0$.

Proposition 2 *If $m \ge 1$ and $n \ge 0$, then $D_n(m) = 2^n C_n\left(\frac{1}{2}, m\right)$.*

Proof:

$$2^n C_n\left(\frac{1}{2}, m\right) = 2^n \sum_{k=1}^{m} (-1)^{m-k}\left(k - \frac{1}{2}\right)^n = \sum_{k=1}^{m} (-1)^{m-k}(2k-1)^n = D_n(m).$$

Proposition 3 *If $m \ge 1$ and $n \ge 0$, then*

$$D_n(m) = \sum_{k=0}^{n-1} \binom{n}{k} 2^{n-k-1} E_k m^{n-k} + \frac{1-(-1)^m}{2} E_n.$$

Proof: Using the previous proposition and Equations (3) and (1), we have

$$\begin{aligned} D_n(m) = 2^n C_n\left(\frac{1}{2}, m\right) &= 2^{n-1}\left(E_n\left(\frac{1}{2} + m\right) - (-1)^m E_n\left(\frac{1}{2}\right)\right) \\ &= 2^{n-1}\left(\sum_{k=0}^{n} \binom{n}{k} \frac{E_k}{2^k} m^{n-k} - (-1)^m \frac{E_n}{2^n}\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} 2^{n-k-1} E_k m^{n-k} - (-1)^m \frac{E_n}{2} \end{aligned}$$

$$= \sum_{k=0}^{n-1} \binom{n}{k} 2^{n-k-1} E_k m^{n-k} + \frac{1-(-1)^m}{2} E_n.$$

Lemma 3 *Let $n \geq 0$, $k \geq 1$, a and b be integers with $a \equiv b \bmod 2^k$.*
(a) If a is odd, then $(2n+2^k)(b) \equiv (2n)(a) + 2^k \bmod 2^{k+1}$.
(b) If a is even, then $(2n+2^k)(b) \equiv (2n)(a) \bmod 2^{k+1}$.

Proof: Write $b = a + c2^k$ for some integer c. Then

$$(2n+2^k)(b) = (2n+2^k)(a+c2^k) \equiv (2n)(a) + a2^k \bmod 2^{k+1}.$$

(a) If a is odd, then $a2^k \equiv 2^k \bmod 2^{k+1}$.
(b) If a is even, then $a2^k \equiv 0 \bmod 2^{k+1}$.

Theorem 6 *For all integers $n \geq 0$ and $k \geq 0$ we have*
$E_{2n} \equiv E_{2n+2^k} + 2^k \bmod 2^{k+1}$.

Proof: Let $m = 1$ in Proposition 3. Then

$$1 = D_n(m) = \sum_{i=0}^{n-1} \binom{n}{i} 2^{n-i-1} E_i + E_n$$

for $n \geq 0$. Replace i by $n-j$ in this formula and find that

$$1 = E_n + \sum_{j=1}^{n} \binom{n}{j} 2^{j-1} E_{n-j}$$

for $n \geq 0$. Replace n first by $2n$ and then again by $2n+2^k$ to get

$$E_{2n} + \sum_{j=1}^{2n} \binom{2n}{j} 2^{j-1} E_{2n-j} = E_{2n+2^k} + \sum_{j=1}^{2n+2^k} \binom{2n+2^k}{j} 2^{j-1} E_{2n+2^k-j},$$

since both sides equal 1. We can rewrite this as

$$E_{2n} = E_{2n+2^k} + \sum_{j=1}^{2n+2^k} 2^{j-1} \left(\binom{2n+2^k}{j} E_{2n+2^k-j} - \binom{2n}{j} E_{2n-j} \right) \quad (5)$$

because $\binom{2n}{j} = 0$ when $j > 2n$. We may ignore the terms with odd j in (5) because $E_{2i+1} = 0$ for all $i \geq 0$. We will show that each term with even j in the sum in (5) is divisible by 2^{k+1}, except the term with $j = 2$, which we will show is $\equiv 2^k \bmod 2^{k+1}$.

We now prove the theorem by induction on k. For $k = 0$ it says $E_{2n} \equiv E_{2n+1} + 1 \bmod 2$. This is true because $E_{2n+1} = 0$ and E_{2n} is odd.

Now let $k \geq 1$ and assume that $E_{2n} \equiv E_{2n+2^{k-1}} + 2^{k-1} \bmod 2^k$. If $k \geq 2$, then also by induction $E_{2n+2^{k-1}} \equiv E_{2n+2^k} + 2^{k-1} \bmod 2^k$, so that

$$E_{2n} \equiv E_{2n+2^{k-1}} \bmod 2^k. \tag{6}$$

In fact, (6) holds also when $k = 1$, since every E_{2n} is odd and $E_{2n+1} = 0$.

The general term in the sum in (5) is

$$\frac{2^{j-1}}{j!}\{(2n + 2^k)(2n + 2^k - 1)\cdots(2n + 2^k - j + 1)E_{2n+2^k-j}$$
$$- (2n)(2n - 1)\cdots(2n - j + 1)E_{2n-j}\}. \tag{7}$$

By Lemma 2, $2^{j-1}/j!$ is a 2-integer, and it equals 1 when $j = 2$. Also, $2n + 2^k - i \equiv 2n - i \bmod 2^k$ for each i. With (6) we have for each even j

$$(2n + 2^k - 1)(2n + 2^k - 3)\cdots(2n + 2^k - j + 1)E_{2n+2^k-j}$$
$$\equiv (2n - 1)(2n - 3)\cdots(2n - j + 1)E_{2n-j} \bmod 2^k.$$

Each side of this congruence is an odd number. We now multiply both sides by the even factors in (7). Multiply the congruence by the congruent even numbers $2n + 2^k - 2i$, $2n - 2i$, one on each side, for each i, and use Lemma 3. When $j = 2$, there is just one even factor on each side, we use Lemma 3(a) once, and the number in (7) is $\equiv 2^k \bmod 2^{k+1}$. When $j > 2$, there is more than one even factor on each side, we use Lemma 3(a) once, Lemma 3(b) at least once, and the general term in (7) is divisible by 2^{k+1}. This proves the theorem.

Corollary 1 *The set* $\{E_0, E_2, \ldots, E_{2^k-2}\}$ *forms a reduced set of residues modulo* 2^k *for* $k \geq 1$.

Proof: Use induction. For $k = 1$, $\{E_0\} = \{1\}$ is an RSR modulo 2^1. Assume true for k and prove for $k+1$. By the theorem, $E_{2n+2^k} \equiv E_{2n} + 2^k \bmod 2^{k+1}$ for $n = 0, 1, \ldots, 2^{k-1} - 1$. Therefore the statement holds for $k + 1$.

Theorem 5 and Corollary 1 were stated without proof by Sylvester [31, 33, 30, 32] in 1861. A few years later, Stern [29] gave brief sketches of proofs of these two results and of Theorem 6. In 1910, Frobenius [15] amplified Stern's sketches of these proofs. Ernvall [13] in 1979 said he couldn't understand Frobenius' outline of the proofs and gave his own proofs using the umbral calculus. The case $e = 0$ of Theorem 5 was proved by Ely [11] and mentioned by Nielsen [21]. These works of Sylvester, Stern and Ely are noted by Saalschütz [26]. Proposition 2 is in Nielsen [21]. Our proofs of Theorems 4, 5 and 6 have the p-adic flavor of proofs of similar statements for the Bernoulli numbers in Johnson [17].

References

[1] John Couch Adams. Table of the first sixty-two numbers of Bernoulli. *J. Reine Angew. Math.*, 85:269–272, 1878.

[2] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993.

[3] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*. Amer. Math. Soc., Providence, 1988.

[4] J. P. Buhler, R. E. Crandall, R. Ernvall, and T. Metsänkylä. Irregular primes and cyclotomic invariants to four million. *Math. Comp.*, 61:151–153, 1993.

[5] J. P. Buhler, R. E. Crandall, R. Ernvall, T. Metsänkylä, and A. Shokrollahi. Irregular primes and cyclotomic invariants to twelve million. *J. Symbolic Computation*, (to appear).

[6] J. P. Buhler, R. E. Crandall, and R. W. Sompolski. Irregular primes to one million. *Math. Comp.*, 59:717–722, 1992.

[7] L. Carlitz. A note on Euler numbers and polynomials. *Nagoya Math. J.*, 7:35–43, 1953.

[8] L. Carlitz and J. Levine. Some problems concerning Kummer's congruences for the Euler numbers and polynomials. *Trans. Amer. Math. Soc.*, 96:23–37, 1960.

[9] Thomas Clausen. Lehrsatz aus einer Abhandlung über die Bernoullischen Zahlen. *Astronomische Nachrichten*, 17:351–352, 1840.

[10] R. E. Crandall. *Topics in Advanced Scientific Computation.* TELOS/Springer-Verlag, Santa Clara, CA, 1996.

[11] G. S. Ely. Some notes on the numbers of Bernoulli and Euler. *Amer. J. of Math.*, 5:337–341, 1882.

[12] R. Ernvall and T. Metsänkylä. Cyclotomic invariants and E-irregular primes. *Math. Comp.*, 32(142):617–629, 1978.

[13] Reijo Ernvall. Generalized Bernoulli numbers, generalized irregular primes, and class number. *Ann. Univ. Turku. Ser. A*, I(178), 1979. 72 pages.

[14] L. Euler. *Institutiones Calculi Differentialis.* Petersberg, 1755.

[15] F. G. Frobenius. Über die Bernoullischen Zahlen und die Eulerschen Polynome. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, pages 809–847, 1910. Also in Gesammelte Abhandlungen III, 1968, Springer-Verlag, pages 440–478.

[16] K. Iwasawa. A class number formula for cyclotomic fields. *Ann. Math.*, 76:171–179, 1962.

[17] Wells Johnson. p-adic proofs of congruences for the Bernoulli numbers. *J. Number Theory*, 7:251–265, 1975.

[18] Donald E. Knuth and Thomas J. Buckholtz. Computation of tangent, Euler, and Bernoulli numbers. *Math. Comp.*, 21:663–688, 1967.

[19] E. E. Kummer. Über eine allgemeine Eigenschaft der rationalen Entwickelungscoëfficienten einer bestimmten Gattung analytischer Functionen. *J. Reine Angew. Math.*, 41:368–372, 1851.

[20] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. Math.*, 126:649–673, 1987.

[21] Niels Nielsen. *Traité Élémentaire des Nombres de Bernoulli.* Gauthier-Villars, Paris, 1923.

[22] M. Ohm. Etwas über die Bernoulli'schen Zahlen. *J. Reine Angew. Math.*, 20:11–12, 1840.

[23] C. Pomerance. The quadratic sieve factoring algorithm. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology, Proceedings of EUROCRYPT 84*, volume 209 of *Lecture Notes in Computer Science*, pages 169–182, Berlin, Heielberg, New York, 1985. Springer-Verlag.

[24] J. L. Raabe. Zurückführung einiger Summen und bestimmten Integrale auf die Jacob-Bernoullische Function. *J. Reine Angew. Math.*, 42:348–367, 1851.

[25] P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York, 1979.

[26] L. Saalschütz. *Vorlesungen über die Bernoullischen Zahlen.* Springer-Verlag, Berlin, 1893.

[27] I. Sh. Slavutskii. Staudt and arithmetical properties of Bernoulli numbers. *Historica Sci. (2)*, 5:69–74, 1995.

[28] I. Sh. Slavutskii. About von Staudt congruences for Bernoulli numbers. *Comment. Math. Univ. St. Paul*, 48:137–144, 1999.

[29] M. A. Stern. Zur Theorie der Eulerschen Zahlen. *J. Reine Angew. Math.*, 79:67–98, 1875.

[30] J. J. Sylvester. Addition à la précédente note. *C. R. Acad. Sci., Paris*, 52:212–214, 1861.

[31] J. J. Sylvester. Note on the numbers of Bernoulli and Euler, and a new theorem concerning prime numbers. *Phil. Magaz.*, 21:127–136, 1861.

[32] J. J. Sylvester. Note relative aux communications faites dans les séances de 28 Janvier et 4 Fèvrier 1861. *C. R. Acad. Sci., Paris*, 52:307–308, 1861.

[33] J. J. Sylvester. Sur une propriété de nombres premiers qui se rattache au dernier théorème de Fermat. *C. R. Acad. Sci., Paris*, 52:161–163, 1861.

[34] K. G. C. von Staudt. Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend. *J. Reine Angew. Math.*, 21:372–374, 1840.

[35] K. G. C. von Staudt. *De numeris Bernoullianis, I, II.* Junge, Erlangen, 1845.

[36] S. S. Wagstaff, Jr. The irregular primes to 125000. *Math. Comp.*, 32(142):583–591, 1978.

Table 1: Bernoulli numerators $|N_n|$ factored

n	Prime factorization of $|N_n|$
60	2003·5549927·109317926249509865753025015237911
62	31·157·266689·329447317·28765594733083851481
64	1226592271·87057315354522179184989699791727
66	11·839·159562251828620181390358590156239282938769
68	17·37·101·123143·1822329343·5525473366510930028227481
70	5·7·688531·20210499584198062453·3090850068576441179447
72	3112655297839·1872341908760688976794226499636304357567811
74	37·923038305114085622008920911661422572613197507651
76	19·58231·22284285930116236430122855560372707885169924709
78	13·787388008575397·33364652939596337·1214698595111676682009391
80	631·10589·5009593·141795949·P39
82	41·4003·38189·P51
84	233·271·68767·167304204004064919523·P37
86	43·541·21563·P55
88	11·307·2682679·P60
90	5·587·1758317910439·P57
92	23·587·108023·P63
94	47·467·1499·2459153·4217126617741589575995641·P34
96	7823741903·4155593423131·10017952436526113· ·96454277809515481·P25
98	7·7·2857·3221·1671211·9215789693276607167·P43
100	263·379·28717943·6567717169275556482181133·P45
102	17·59·827·17833331·86023144558386407· ·299116358909830276447443337·P28
104	13·37·776253902057299·6644689804135385589700423·P45
106	53·3967·37217·77272435237709·P65
108	656884664663·23657486502844933·P69
110	5·157·76493·150235116317549231·36944818874116823428357691·P44
112	7·887569·8065483·P86
114	19·P97
116	29·7559·7438099·6795944986967·P77
118	59·P100
120	6495690221·8070196213·P93
122	61·1545314586433142560447·1545923474257037240728199709913·P54
124	31·67·74747·162263·14066893·8262971607841· ·3498285428145163·16743250272239551·P45
126	103·409·216363744721·P102
128	35089·5953097·12349588663·13349390911530343· ·6996505560116602097773394576621473·P46
130	5·13·149·463·2264267·3581984682522167·P92
132	11·804889·10462099·P112

Table 2: Large prime factors of Bernoulli numerators $|N_n|$

n	Large prime factors of $|N_n|$
134	338420464438865099·600544027788809384905134504624 2759·P65
136	29835096585483934621·P98
138	554744941981·756906736720877·
	·995959666194215326642640313557460384 7379·P48
140	44124706530665069·4991909895521399443224316 2077·P68
142	1117819549084794843 83981·P105
144	P135
146	22639970526343·67261597027838 54797·
	·3799632499854774053969152 8067877·
	·17548211726562669269669237 16442469·P34
148	4975417507662031677157·
	·12488634364608605230327 49·P84
150	5810708205829·21664796739499531040947·
	·24097950820156725667332187 56037·P72
152	3720341037827029338655181363717044961·
	·378357160740584268907255965503041181 96498159·P52
154	384785986561·C123
156	16760414993553486506 4907·
	·94884267483295622200143616179947·P101
160	40094692599177383·12830086712891890983430059948563·
	·174482650542336239004683326605040370 3791289·P62
164	104386532651·2903061743891·9898920431428993·C117
166	311318618909·37074748512889·
	·605190683329889640846518910 32717·
	·11709228761805923962023525960553218 9619·P52
168	19254163575306510187·10094494587919631151637·C128
170	751612064207·P154
172	P174
174	6659961564676431900928667503·C137
176	333026571343·110783038328477·124813394943812621·C138
178	129180506448277·1823634234826012967·39326836920802601519·P129
180	249829228470043·2076252436787489535833·
	·4241477436592626145879·P127
182	73107144475261423·311089841618633327·362702761564874666647 7·
	·21221741142274196480934616 01·
	·83276165458323300429587071706402939815926 73849·P59
184	21983088204089362967·P169
186	922966808867·9161904079472101·C156
190	60860762760882373·1742620927079710201045387 09609·C152
196	5827361715660128207224263 7946609·C173
198	723357738211·P201
200	5370056528687·C204

Table 3: Large prime factors of Bernoulli numerators $|N_n|$

n	Large prime factors of $|N_n|$
202	85704723183916799·C173
204	9131578873975602379·P207
206	4134128959054219·28391723373218209·40842843991225271078320l· ·479477942782400905131851073960379649З· ·3705636735000917624663544925511551624891·P77
216	P239
218	4986305046278328485613904846831·C175
220	792913356669011·C224
222	270574469649607096339·C229
224	67653517083823116668886121·13568731058606497266528850207·P187
226	226941007255811687·C229
230	9487561145259955585249403·C234
232	2483032145171·259051164055671909270473820520219·P225
234	48237362885215689907·C222
236	504680422913·14656891523109995294576720509429987·C219
238	30079831621249·C258
240	26230095767160160157·C260
242	49675522089194103641917241·C236
246	1015348391695196501·C267
248	115134703427104257294711265272763·C240
252	2028290804799829·650932177698080567099· ·130625066385309173899099708579· ·754223542032486571885216433401349· ·1000993741524774643539942570884595839·C171
258	1236523928730271·C292
262	63379712903619825709847·P278
266	167825382335090242001·1727816222222026922465407· ·1571264305785183471309381325703·C216
270	2539833907837164114167·P306
274	21804608848811·201500345265433·31628480989746829· ·3277838401217446489·25729084799117836987901· ·892008372912807309877541·C222
276	116773511307223·9280481761112414180447102368597·C293
280	136100780239·C338
282	4525048629470223385658435650031·C311
284	792213846555737·C331
286	8812943587829·16865476527940273· ·34000751682694166738635652417·C285
288	1259554461969878619108227·C328
292	P359
296	146409753143342542769·C351
298	371472263795653589766634977803·P332
300	7985787872578979·C352

Table 4: Euler numbers $|E_n|$ factored

n	Prime factorization of $|E_n|$
40	5·5·41·763601·52778129·359513962188687126618793
42	137·5563·13599529127564174819549339030619651971
44	5·587·32027·9728167327·36408069989737·238716161191111
46	19·285528427091·1229030085617829967076190070873124909
48	5·13·17·5516994249383296071214195242422482492286460673697
50	5639·1508047·10546435076057211497·67494515552598479622918721
52	5·31·53·1601·2144617·537569557577904730817·P24
54	43·2749·3886651·78383747632327·P36
56	5·29·5303·7256152441·52327916441·2551319957161·P26
58	1459879476771247347961031445001033·P34
60	5·5·13·47·61·6821509·14922423647156041·P42
62	101·6863·418739·1042901·P56
64	5·17·19·25349·85297·P65
66	61·105075119·508679461·155312172341·P51
68	5·2039·66041·29487071944189·15138431327918641·P45
70	353·25864370560363360277012341011159·P54
72	5·13·37·73·2341·4014623·24259423·306015870754393337·P51
74	193·34629826749613·4207222848740394629·
	·22060457167870794468746201·P34
76	5·145007·3460859370585503071·581662827280863723239564386159·P43
78	2740019561103910291228417123054994825316979387·P55
80	5·5·17·41·7701306020743·3572363603188902175396213·P62
82	19·31·4395659·P98
84	5·13·29·4397·739762335239015186706527735192795520726707·P62
86	311·390751·46053168570671·P92
88	5·89·1019·588528876550967927·16292380848703930709213·P72
90	307·C119
92	5·67·7096363493·7308346963823·120476813565517·P85
94	53089·20609829625906839913745698187·
	·180986288780569828566819992453·P66
96	5·13·17·43·79·97·835823·2233081·1951860271597317997069749059·
	·9416370608392625586845089085196635167·P47
98	71·376003429·5160267661·4363907262506552373343·P94
100	5·5·5·19·101·C134
102	8647·C139
104	5·53·761·2477·P138
106	47·4858416191·98985829942673·
	·1150887066548393492521971151372616707·P88
108	5·13·37·109·1462621·8445961·4675063901·C125
110	509053·116904299·134912677·748079839770433·P120
112	5·17·29·31·113·8185757·617575481323·1522046069820268709·
	·265053146030428876430329·P94

Table 5: Large prime factors of Euler numbers $|E_n|$

n	Large prime factors of $|E_n|$
114	5290253211544727·22557103319451713·
	·25659486698674613133182155567·
	·118972684453835135392634192556273454718187595705343·P52
116	1098948437923935829829·17698520871521406115634951924463689·
	·116619065933163530588469118477095110617775 23·P69
118	86611938909696635972683149781·C142
124	545893110893363273374339·C137
126	44305294819613·16723717485156209220 1·P128
128	91486803609919·33397018471037747·
	·38280927951817207·1823694188853227904949904627·
	·25218189671884291383279399150744135824 9·P64
134	321639994822891·21407431771728232601749801895 3·P148
136	P200
138	12254459673349·34356165690119899·P157
140	P199
142	2978734769·8557612247·P197
144	978576085558923501179·17051321837018915595804889137 1·P149
146	P213
148	238661068231279·C202
150	13621373428254587·
	·1113819739992602282822381674313355854330 59·C168
152	1805155617412973535918 1·39576664495302675105890 53·
	·43832133409518382465829470936 7·C149
154	139668927262709710013·C210
156	227071134239·P198
158	5519160811451003·C220
162	174175655449·C242
164	6348884877435650273054306063 3·C209
166	50150236900098278077·C214
168	86771436435012390277·C230
170	70727223023077·1034326231547973051559·P239
172	743155422133·2840083403239·C243
180	6923483330327017·C269
184	280438957970679763 3·C284
186	22658461432253·54342802734882461·
	·1086110887390889008410968159777·C229
190	559570609330768709·6386014734599369410586902768943·C265
192	1469840300183·68957665149611180 59·
	·1269672106384218692615790692911·C249
194	28024555486506389·24364377502043108048 41·P278
198	2507798651531·4963930521045390100943203 1·C277
200	16640782677056849·C306