For every prime $p > 2$ and every prime divisor d of $p-1$ for which $(p-1)/d$ is *odd*, we define a "Bernoulli number" $B(p,d)$ as follows.

For every pair (p,d) as above we put $f = 2$ when $d = p-1$ and $f = p$ when d is a power of 2. In the rare cases when $d = p-1$ is itself a power of 2, we let $f = 2p$. In *all* other cases we let $f = 1$.

Then

$$B(p,d) = f \cdot \prod_{\substack{0<k\leq d \\ \gcd(k,d)=1}} -\frac{1}{2p}\sum_{j=1}^{p-1}[g^j \pmod p]\exp(\frac{2\pi ijk}{d}).$$

Here $i \in \mathbf{C}$ is a square root of -1 and g denotes a primitive root modulo p. By $[g^j \pmod p]$ we denote the unique integer between 0 and p that is congruent to g^j modulo p.

In 1978 D.H. Lehmer and J.M. Masley presented a table with the numbers $B(p,d)$ for $p \leq 509$. Of most of these numbers the prime factorization was given, but their table contains 22 unfactored composite numbers. These were the Bernoulli numbers $B(p,p-1)$ for certain primes $p \geq 233$.

The 22 numbers were factored by several people. First Peter Montgomery (PM) found the small factors in the spring of 1986, using the elliptic curve method and its $\mathbf{G}_m$-analogues, the $p-1$ and $p+1$ methods. Only the 12 digit prime factor of $B(503,502)$ was found by means of Pollard's ρ-method. Montgomery was given a hand by Bob Silverman (BS) who found some of the larger prime factors by means of the Multiple Polynomial Quadratic Sieve. A list of nine composite numbers remained, In 1990 Herman te Riele (HtR) used the same algorithm to factor five numbers from the list of 69, 74, 75, 79 and 79 decimal digits respectively. A year later, using the elliptic curve method, Arjen Lenstra (AL) found three prime factors of 24, 27 and 28 digits respectively. The last number left was a 103 digit factor of the number $B(467,466)$. Using the Quadratic Sieve it was factored by Arjen Lenstra into a product of two primes of 49 and 55 digits respectively. In all cases the factors were proved to be primes by means of Atkin's algorithm.

We list the various factorizations of $B(p,d)$ in the Table. By p_n we denote a prime factor of n decimal digits. The order in which the initials are given corresponds to the order of the prime factors found.

Table.

p			p		
233	$p_{14} \cdot p_{29}$	PM	419	$p_{16} \cdot p_{30} \cdot p_{49}$	PM, HtR
269	$p_{16} \cdot p_{31}$	PM	433	$p_{14} \cdot p_{34}$	PM
317	$p_{25} \cdot p_{49}$	HtR	439	$p_{11} \cdot p_{21} \cdot p_{23} \cdot p_{24}$	PM, PM, PM
337	$p_{13} \cdot p_{15} \cdot p_{15}$	PM, PM	449	$p_{18} \cdot p_{84}$	PM
359	$p_{13} \cdot p_{30} \cdot p_{45}$	PM, HtR	463	$p_{18} \cdot p_{21} \cdot p_{25}$	PM, BS
379	$p_{22} \cdot p_{24}$	BS	467	$p_{19} \cdot p_{49} \cdot p_{55}$	PM, AL
383	$p_{19} \cdot p_{24} \cdot p_{46}$	PM, HtR	479	$p_{20} \cdot p_{27} \cdot p_{70}$	PM, AL
389	$p_{24} \cdot p_{60}$	AL	487	$p_{30} \cdot p_{49}$	HtR
397	$p_{8} \cdot p_{26} \cdot p_{27}$	PM, BS	499	$p_{15} \cdot p_{18} \cdot p_{47}$	PM, PM
401	$p_{16} \cdot p_{18} \cdot p_{31}$	PM, PM	503	$p_{12} \cdot p_{14} \cdot p_{112}$	PM, PM
409	$p_{12} \cdot p_{52}$	PM	509	$p_{16} \cdot p_{28} \cdot p_{101}$	PM, AL