A theorem of Charles Babbage's extended

F.L. Bauer [0] told me that Charles Babbage has shown that
\[
\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}
\]
if and only if \( p \) is an odd prime. He furthermore transmitted to me his conjecture that
\[
\binom{(k+1)p-1}{p-1} \equiv 1 \pmod{p^3}
\]
for natural \( k \) and prime \( p \geq 5 \), which will be proved in this note.

**Conventions** All through this note
- \( k \) is a natural number
- \( p \) is a prime satisfying \( p > 5 \)
- \( n \) satisfies \( p = 2n + 1 \)
- \( F \) satisfies \( F = (p-1)! \)
- \((S\text{ dummies} : \text{range} : \text{term})\) is the format used to denote summation
- \((P\text{ dummies} : \text{range} : \text{factor})\) is the format used to denote multiplication. (End of Conventions)

On account of the definition of binomial coefficients, the demonstrandum is equivalent to
\[
\binom{p}{1 \leq i < p : kp+1} / F \equiv 1 \pmod{p^3}
\]
or equivalently, since \( F \) has no factor \( p \),
\[
\binom{p}{1 \leq i < p : kp+i} \equiv F \pmod{p^3}.
\]

To begin with, we therefore expand the left-hand side in powers of \( kp \). This yields
\[
\binom{p}{1 \leq i < p : kp+i} = F + C \cdot (kp) + D \cdot (kp)^2 + \text{higher powers of } kp
\]
with \[ C = (\forall i : 1 \leq i < p : F/i) \]
and \[ D = (\forall i,j : 1 \leq i,j < p : F/ij) \]

In view of the expansion, the demonstrandum follows from (the stronger)

(0) \[ C \equiv 0 \pmod{p^2} \]
and
(1) \[ D \equiv 0 \pmod{p} \]

Let us tackle proof obligation (0) first. We observe
\[
C
= \{ \text{definition} \}
(\forall i : 1 \leq i < p : F/i)
= \{ \text{splitting the range} \}
(\forall i : 1 \leq i \leq n : F/i) + (\forall i : n < i < p : F/i)
= \{ \text{renaming the second dummy: } i := p-j \}
(\forall i : 1 \leq i \leq n : F/i) + (\forall j : 1 \leq j \leq n : F/(p-j))
= \{ \text{combining summations over equal ranges} \}
(\forall i : 1 \leq i \leq n : F/i + F/(p-i))
= \{ \text{arithmetic} \}
p \cdot (\forall i : 1 \leq i \leq n : F/(i \cdot (p-i)))
\]

Hence, proof obligation (0) can be discharged by demonstrating

(2) \[ (\forall i : 1 \leq i \leq n : F/(i \cdot (p-i))) \equiv 0 \pmod{p} \]

Furthermore we deduce from the above

(3) \[ C \equiv 0 \pmod{p} \]

For the moment we shelve proof obligation (2) and tackle proof obligation (1). To this end we observe - elementary algebra -

(4) \[ C^2 = (\forall i : 1 \leq i < p : F^2/i^2) + 2FD \]
which allows us to rewrite (1):

\[ D \equiv 0 \pmod{p} \]
\[ = \{ 2F \text{ has no factor } p \} \]
\[ 2FD \equiv 0 \pmod{p} \]
\[ = \{ (4) \} \]
\[ C^2 - (\sum_{i=1}^{p} F^{2/i^2}) \equiv 0 \pmod{p} \]
\[ = \{ (3) \} \]
\[ -(\sum_{i=1}^{p} F^{2/i^2}) \equiv 0 \pmod{p} \quad (5) \]

Hence, proof obligation (1) can be discharged by demonstrating (5), which is encouragingly similar to (2), our other remaining proof obligation.

Because both (2) and (5) are congruences modulo \( p \), we now resort to the residue calculus modulo \( p \). In what follows, taking the residue class of a (rational) argument is denoted by surrounding the argument by a pair of square brackets.

Interlude We recall

- for integer arguments \( x \) and \( y \): \([x] \oplus [y] \equiv p | (x-y)\)
  (for "\( a \mid b \)" read "\( a \) divides \( b \)"")
- there are \( p \) distinct residue classes
- addition, subtraction, and multiplication of residue classes is defined by the distribution of the square brackets over these operators, i.e.
  \([x] \oplus [y] = [x+y]\)
  \([x] - [y] = [x-y]\)
  \([x] \cdot [y] = [x \cdot y]\)
- as \( p \) is prime
  \([x] \cdot [y] = [0] \equiv [x] = [0] \lor [y] = [0]\)
as $p$ is prime, the equation in the unknown residue class $z$
$$z: ([x] = [y] \cdot z)$$
has for $[y] \neq [0]$ a unique solution, denoted by $[x]/[y]$.

by letting the square brackets distribute over division as well, i.e.
$$[x]/[y] = [x/y]$$

residue classes for prime $p$ are also assigned to rational fractions $x/y$ with $[y] \neq [0]$.

(End of Interlude.)

We tackle (5) first:

(5)

= \{ definitions of (5) and of residue class \}

\[-(S_i: 1 \leq i < p: F^2/i^2)) = [0]\]

= \{ arithmetic \}

\[-F^2 \cdot (S_i: 1 \leq i < p: 1/i^2)) = [0]\]

= \{ distribution \}

\[-F^2 \cdot (S_i: 1 \leq i < p: 1/i^2)) = [0]\]

= \{ \neg F^2 \neq [0] \}

\[(S_i: 1 \leq i < p: 1/i^2)) = [0]\]

= \{ p = 2n+1 \}

\[(S_i: 1 \leq i \leq n: 1/i^2 + 1/(p-1)^2)) = [0]\]

= \{ distribution \}

\[(S_i: 1 \leq i \leq n: [1/i^2] + [1/(p-1)^2]) = [0]\]

= \{ \ [x/y] = [x/(y-p)] \}

\[(S_i: 1 \leq i \leq n: [1/i^2] + [1/i^2]))) = [0]\]

= \{ distribution \}

\[(S_i: 1 \leq i \leq n: [2/i^2]) = [0]\]

= \{ distribution \}

\[2 \cdot (S_i: 1 \leq i \leq n: [1/i^2]) = [0]\]

= \{ \ [2] \neq [0] \}

(6) \ (S_i: 1 \leq i \leq n: [1/i^2]) = [0]
Now we tackle (2):

(2) \[
\{ \text{definitions of (2) and of residue class}\} \\
\{(1 \leq i \leq n: F/i \cdot (p-i))\} = [0] \\
\{ \text{arithmetic}\} \\
\{-F, \{(1 \leq i \leq n: 1/i \cdot (p-i))\}\} = [0] \\
\{ \text{distribution}\} \\
\{-F, \{(1 \leq i \leq n: 1/i^2 \cdot (p-i))\}\} = [0] \\
\{ \{ -F \neq [0]\} \\
\{(1 \leq i \leq n: 1/i^2 \cdot (p-i))\} = [0] \\
\{ \{ x/y \neq [x/(y-p)]\} \\
(6) \{(1 \leq i \leq n: 1/i^2)\} = [0]
\]

and hence our two still outstanding proof obligations (2) and (5) can both be discharged by showing (6).

Since for integer \( i \) and \( j \)

\[
[i^2] = [j^2] \\
\{ \text{residue calculus}\} \\
[i+j] \cdot [i-j] = [0] \\
\{ \text{p is prime}\} \\
[i+j] = [0] \lor [i-j] = [0]
\]

our \( p = 2n+1 \) residue classes fall apart in \( n \) non-squares, square \([0]\) and \( n \) "positive squares" and for \( i \) ranging over \( 1 \leq i \leq n \), \([i^2]\) ranges over the positive squares.

However, for integer \( i \) and \( j \) with \([ij] \neq [0]\)

\[
[1/i^2] = [1/j^2] \\
\{ \text{residue calculus}\} \\
[i+j] \cdot [i-j] \cdot [1/i^2 j^2] = [0] \\
\{ \{1/i^2 j^2\} \neq [0]\}
\]
\[ [i+j] \cdot [i-j] = [0] \]
\[ = \begin{cases} p \text{ is prime} \\ [i+j] = [0] \lor [i-j] = 0 \end{cases} \]

and, because \( [1/i^2] \neq [0] \), we conclude by the same token that for \( i \) ranging over \( 1 \leq i \leq n \), also \( [1/i^2] \) ranges over the positive squares, and hence

(6)
\[ = \begin{cases} \text{definition of (6) and above remarks} \\ (\sum_{i=1}^{n} [i^2]) = [0] \end{cases} \]
\[ = \begin{cases} \text{distribution} \\ \sum_{i=1}^{n} i^2 = [0] \end{cases} \]
\[ = \begin{cases} \text{algebra} \\ n \cdot (n+1) \cdot (2n+1)/6 = [0] \end{cases} \]
\[ = \begin{cases} \text{2n+1 = p and } \gcd(p,6) = 1 \text{ true} \end{cases} \]

And this concludes the proof.

[0] F.L. Bauer, Private Communication

Austin, 19 October 1986

---

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712 - 1188
United States of America