A theorem of Charles Babbage's extended

F.L. Bauer [0] told me that Charles Babbage has shown that

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^2} \quad \text{if and only if } p \text{ is an odd prime.}$$

He furthermore transmitted to me his conjecture that

$$\binom{(k+1)p-1}{p-1} \equiv 1 \pmod{p^3} \quad \text{for natural } k \text{ and prime } p \geq 5,$$

which will be proved in this note.

<u>Conventions</u> All through this note

- k is a natural number
- p is a prime satisfying $p \geq 5$
- n satisfies $p = 2n+1$
- F satisfies $F = (p-1)!$
- ($\underline{S}$ dummies: range: term) is the format used to denote summation
- ($\underline{P}$ dummies: range: factor) is the format used to denote multiplication.

(End of Conventions)

On account of the definition of binomial coefficients, the demonstrandum is equivalent to

$$(\underline{P}i : 1 \leq i < p : kp+i)/F \equiv 1 \pmod{p^3}$$

or equivalently, since F has no factor p,

$$(\underline{P}i : 1 \leq i < p : kp+i) \equiv F \pmod{p^3} .$$

To begin with, we therefore expand the left-hand side in powers of kp. This yields

$$(\underline{P}i : 1 \leq i < p : kp+i) = F. + C\cdot(kp) + D\cdot(kp)^2 + \text{higher powers of } kp$$

with $\quad C = (\underline{S}\, i : 1 \le i < p : F/i)$
and $\quad D = (\underline{S}\, i,j : 1 \le i < j < p : F/ij)$.

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

(0) $\quad C \equiv 0 \pmod{p^2}$ $\qquad$ and
(1) $\quad D \equiv 0 \pmod{p}$.

Let us tackle proof obligation (0) first. We observe

$$
\begin{array}{ll}
 & C \\
= & \{\text{definition}\} \\
 & (\underline{S}\, i : 1 \le i < p : F/i) \\
= & \{\text{splitting the range}\} \\
 & (\underline{S}\, i : 1 \le i \le n : F/i) + (\underline{S}\, i : n < i < p : F/i) \\
= & \{\text{renaming the second dummy: } i := p-j\} \\
 & (\underline{S}\, i : 1 \le i \le n : F/i) + (\underline{S}\, j : 1 \le j \le n : F/(p-j)) \\
= & \{\text{combining summations over equal ranges}\} \\
 & (\underline{S}\, i : 1 \le i \le n : F/i + F/(p-i)) \\
= & \{\text{arithmetic}\} \\
 & p \cdot (\underline{S}\, i : 1 \le i \le n : F/(i \cdot (p-i)))\ .
\end{array}
$$

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

(2) $\quad (\underline{S}\, i : 1 \le i \le n : F/(i \cdot (p-i))) \equiv 0 \pmod{p}$;

furthermore we deduce from the above

(3) $\quad C \equiv 0 \pmod{p}$.

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

(4) $\qquad C^2 = (\underline{S}\, i : 1 \le i < p : F^2/i^2) + 2FD$,

which allows us to rewrite (1):

$$
\begin{array}{ll}
 & D \equiv 0 \pmod p \\
= & \quad \{ 2F \text{ has no factor } p \} \\
 & 2FD \equiv 0 \pmod p \\
= & \quad \{ (4) \} \\
 & C^2 - (\underline{S} i : 1 \leq i < p : F^2/i^2) \equiv 0 \pmod p \\
= & \quad \{ (3) \} \\
(5) & -(\underline{S} i : 1 \leq i < p : F^2/i^2) \equiv 0 \pmod p \quad .
\end{array}
$$

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.

<u>Interlude</u> We recall

- for integer arguments x and y: $[x] = [y] \equiv p \mid (x-y)$
  (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.

$$
\begin{aligned}
[x] + [y] &= [x+y] \\
[x] - [y] &= [x-y] \\
[x] \cdot [y] &= [x \cdot y]
\end{aligned}
$$

- as p is prime

$$[x] \cdot [y] = [0] \quad \equiv \quad [x] = [0] \lor [y] = [0]$$

- 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:

$$
\begin{array}{ll}
 & (5) \\
= & \quad \{\text{definitions of (5) and of residue class}\} \\
 & [-(\underline{S}i: 1 \leq i < p: F^2/i^2)] = [0] \\
= & \quad \{\text{arithmetic}\} \\
 & [-F^2 \cdot (\underline{S}i: 1 \leq i < p: 1/i^2)] = [0] \\
= & \quad \{\text{distribution}\} \\
 & [-F^2] \cdot [(\underline{S}i: 1 \leq i < p: 1/i^2)] = [0] \\
= & \quad \{[-F^2] \neq [0]\} \\
 & [(\underline{S}i: 1 \leq i < p: 1/i^2)] = [0] \\
= & \quad \{p = 2n+1\} \\
 & [(\underline{S}i: 1 \leq i \leq n: 1/i^2 + 1/(p-i)^2)] = [0] \\
= & \quad \{\text{distribution}\} \\
 & (\underline{S}i: 1 \leq i \leq n: [1/i^2] + [1/(p^2 - 2pi + i^2]) = [0] \\
= & \quad \{[x/y] = [x/(y-p)]\} \\
 & (\underline{S}i: 1 \leq i \leq n: [1/i^2] + [1/i^2]) = [0] \\
= & \quad \{\text{distribution}\} \\
 & (\underline{S}i: 1 \leq i \leq n: [2/i^2]) = [0] \\
= & \quad \{\text{distribution}\} \\
 & [2] \cdot (\underline{S}i: 1 \leq i \leq n: [1/i^2]) = [0] \\
= & \quad \{[2] \neq [0]\} \\
(6) & (\underline{S}i: 1 \leq i \leq n: [1/i^2]) = [0]
\end{array}
$$

Now we tackle (2):

$$
\begin{array}{ll}
 & (2) \\
= & \{\text{definitions of (2) and of residue class}\} \\
 & [(\underline{S}i: 1 \leq i \leq n: F/i\cdot(p-i))] = [0] \\
= & \{\text{arithmetic}\} \\
 & [-F\cdot(\underline{S}i: 1 \leq i \leq n: 1/i\cdot(i-p))] = [0] \\
= & \{\text{distribution}\} \\
 & [-F]\cdot(\underline{S}i: 1 \leq i \leq n: [1/(i^2-ip)]) = [0] \\
= & \{[-F] \neq [0]\} \\
 & (\underline{S}i: 1 \leq i \leq n: [1/(i^2-ip)]) = [0] \\
= & \{[x/y] = [x/(y-p)]\} \\
(6) & (\underline{S}i: 1 \leq i \leq n: [1/i^2]) = [0]
\end{array}
$$

,

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

Since for integer i and j

$$
\begin{array}{ll}
 & [i^2] = [j^2] \\
= & \{\text{residue calculus}\} \\
 & [i+j]\cdot[i-j] = [0] \\
= & \{p \text{ is prime}\} \\
 & [i+j] = [0] \vee [i-j] = [0]
\end{array}
$$

,

our p $(= 2n+1)$ residue classes fall apart in n nonsquares, 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 $[ij] \neq [0]$

$$
\begin{array}{ll}
 & [1/i^2] = [1/j^2] \\
= & \{\text{residue calculus}\} \\
 & [i+j]\cdot[i-j]\cdot[1/i^2j^2] = [0] \\
= & \{[1/i^2j^2] \neq [0]\}
\end{array}
$$

$$
\begin{aligned}
& [i+j]\cdot[i-j] = [0] \\
= \quad & \{ p \text{ is prime} \} \\
& [i+j] = [0] \ \vee\ [i-j] = 0
\end{aligned}
$$

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

$$
\begin{aligned}
& (6) \\
= \quad & \{ \text{definition of } (6) \text{ and above remarks} \} \\
& (\underline{S} i : 1 \le i \le n : [i^2]) = [0] \\
= \quad & \{ \text{distribution} \} \\
& [(\underline{S} i : 1 \le i \le n : i^2)] = [0] \\
= \quad & \{ \text{algebra} \} \\
& [\ n\cdot(n+1)\cdot(2n+1)/6\ ] = [0] \\
= \quad & \{ 2n+1 = p \ \text{ and } \ \gcd(p,6) = 1 \} \\
& \mathit{true} .
\end{aligned}
$$

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