F.L. Bauer's Conjecture is F.L. Bauer's Theorem

During the recent Marktoberdorf Summer School — to be precise: during the dinner at the end of the Excursion on Wednesday 6 August 1986 — Fritz Bauer conveyed to me the following conjecture:

For positive integer k and prime p exceeding 3:

$$\binom{k\cdot p}{p}/k - 1 \quad \text{is a multiple of } p^3 \ .$$

*   *
   *

Replacing k by $k+1$, we have to establish for natural k

$$\binom{(k+1)\cdot p}{p}/(k+1) - 1 \quad \text{is a multiple of } p^3 \ ,$$

or, by virtue of the definition of the binomial coefficient

$$\frac{(\underline{P}\, i : 1 \le i < p : (k\cdot p + i))}{(\underline{P}\, i : 1 \le i < p : i)} - 1 \quad \text{is a multiple of } p^3 \ ,$$

or, equivalently,

$$(\underline{P}\, i : 1 \le i < p : (k\cdot p + i)) - (p-1)! \quad \text{is a multiple of } p^3 .$$

To this end, we develop the product into powers of $k.p$:

$$(\underline{P}\, i : 1 \le i < p : (k\cdot p + i))$$

$$= \ (p-1)! \quad +$$

$k \cdot p \cdot (\underline{S}\, i : 1 \le i < p : (p-1)!/i)$ +

$(k \cdot p)^2 \cdot (\underline{S}\, i,j : 1 \le i < j < p : (p-1)!/(i \cdot j))$ +

higher powers of $k \cdot p$

The demonstrandum thus follows from the following two lemmata:

Lemma 0: For prime p such that $p > 3$

$$(\underline{S}\, i : 1 \le i < p : (p-1)!/i) \ \underline{\text{mod}}\ p^2 = 0 \quad .$$

Lemma 1: For prime p such that $p > 3$

$$(\underline{S}\, i,j : 1 \le i < j < p : (p-1)!/(i \cdot j)) \ \underline{\text{mod}}\ p = 0 \quad .$$

In these summations we are going to combine terms whose denominators sum up to (a multiple of) p. In the following, n is given by

$$2 \cdot n + 1 = p \quad .$$

For Lemma 0, this allows us to rewrite

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

and, consequently, the proof obligation of Lemma 0 can be discharged by showing Lemma 2:

<u>Lemma 2</u> For prime p such that $p>3$ (and $2\cdot n+1=p$)

$$(\underline{S}i: 1\le i\le n: (p-1)!/(i\cdot(p-i)))\ \underline{mod}\ p=0$$

or, equivalently,

$$(\underline{S}i,j: 1\le i<j<p \ \wedge\ i+j=p: (p-1)!/(i\cdot j))\ \underline{mod}\ p=0 \quad .$$

From the last rewriting we see that Lemma 2 is concerned with a subset of the terms summed in Lemma 1. Before pursuing Lemma 2, let us inspect the remaining terms in Lemma 1. Since

$$i+j=p \ \vee\ i+j<p \ \vee\ i+j>p$$

we analyse

$$
\begin{array}{ll}
 & (\underline{S}i,j: 1\le i<j<p \ \wedge\ i+j<p: (p-1)!/(i\cdot j)) \\
= & \{\text{arithmetic}\} \\
 & (\underline{S}i,j: 1\le i<j<p-i: (p-1)!/(i\cdot j)) \\
= & \{\text{nesting summations}\} \\
 & (\underline{S}i: 1\le i\le n: (\underline{S}j: i<j<p-i: (p-1)!/(i\cdot j)))
\end{array}
$$

in which the inner summation can be rewritten

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

We trust that, after the above, the reader believes as well that the terms with $i+j>p$ add up to a multiple of p. Hence also the proof obligation of Lemma 1 has been reduced to proving Lemma 2.

On the proof of Lemma 2 I spent at least five vain hours looking for a nice combinatorial argument in the style of my proof of Wilson's Theorem (EWD742). [This was psychologically very strange because all the time I knew that the effort was ill-directed since ruling out the primes 2 and 3 would not fit in it. And yet I tried for more than five hours .....]

Eventually I found an argument by considering
(i) that Lemma 2 is the same as

"computing $(\underline{S}i: 1 \le i < n: 1/(i\cdot(p-i)))$ by finding the common denominator leads to a fraction with a numerator that is a multiple of p"

(ii) the computation under (i) can be done while reducing all intermediate results modulo p.

So much for the heuristics.

For given p we consider the p "restclasses", i.e. the infinite sets of integers such that any two of them differ by a multiple of p. For any rational fraction x/y such that $y \;\underline{\mathrm{mod}}\; p \ne 0$ we define the rest class $[x/y]$ by

$$[x/y] = \{z \mid x \;\underline{\mathrm{mod}}\; p = y\cdot z \;\underline{\mathrm{mod}}\; p\}$$

(On account of $y \underline{\text{mod}}\ p \neq 0$ and p being prime it is not difficult to see that the equation

$$y : (x \ \underline{\text{mod}}\ p = y \cdot z \ \underline{\text{mod}}\ p)$$

has solutions that form a rest class.)

We can now define an arithmetic on rest classes by

$$[a] + [b] = [a+b] \qquad [a] - [b] = [a-b]$$
$$[a] \cdot [b] = [a \cdot b]$$
$$[a] / [b] = [a/b] \quad \text{provided } [b] \neq [0] \quad ,$$

and may use

$$[a] = [b] \equiv [a] - [b] = [0]$$
$$[x/y] = [(x+p)/y]$$
$$[x/y] = [x/(y+p)]$$
$$[x] \cdot [y] = [0] \equiv [x] = [0] \vee [y] = [0] \quad \text{etc.}$$

The important thing to observe is that among the p rest classes there are $n+1$ "squares", i.e. rest classes of the form $[x^2]$. They are $[0]$, with $[0]$ as its only square root and the n "positive squares" $[i^2]$ for $1 \leq i \leq n$ with $[i]$ and $[p-i]$ as their square roots. From

$$\begin{aligned} & [i^2] = [j^2] \\ = \ & [i^2 - j^2] = [0] \\ = \ & [i-j] = [0] \vee [i+j] = [0] \end{aligned}$$

we conclude that $[0]$ and the n positive squares are all different.

After these preliminaries we are ready to attack Lemma 2

$$
\begin{aligned}
& [(\underline{S}i : 1 \le i \le n : (p-1)!/(i\cdot(p-i)))] \\
= \; & [(p-1)!]\cdot(\underline{S}i : 1 \le i \le n : [1/(i\cdot(p-i))]) \\
= -\; & [(p-1)!]\cdot(\underline{S}i : 1 \le i \le n : [1/i^2]) \\
= -\; & [(p-1)!]\cdot(\underline{S}i : 1 \le i \le n : [i^2]) && {*)} \\
= -\; & [(p-1)!]\cdot[(\underline{S}i : 1 \le i \le n : i^2)] \\
= -\; & [(p-1)!]\cdot[n\cdot(n+1)\cdot(2\cdot n+1)/6] \\
= \; & [0] && {**)}
\end{aligned}
$$

*) $1 \le i \le j \le n \;\wedge\; [1/i^2] = [1/j^2]$
$= 1 \le i \le j \le n \;\wedge\; [(i^2 - j^2)/i^2\cdot j^2] = [0]$
$\Rightarrow i = j$, hence it is a sum of n different squares. As $[0]$ is not among them, it is the sum of the n positive squares.

**) Remember $2\cdot n+1 = p$; $n\cdot(n+1)\cdot p/6$ has a factor p for prime $p \geq 5$.

Austin 22 August 1986

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin TX 78712-1188
USA