manuscripta math. 56, 67 - 70 (1986)

manuscripta mathematica

On Krasner's Criteria for the First Case of Fermat's Last Theorem

Andrew Granville

The First Case of Fermat's Last Theorem is said to be true for prime p if there do not exist integers a_1, a_2, a_3 for which

$$a_1^p + a_2^p + a_3^p = 0 \quad \text{and} \quad p \nmid a_1 a_2 a_3 \tag{1}p$$

In 1857, Kummer (see [4], pgs 115-125) established that if a_1, a_2, a_3 satisfy (1)p, then

$$B_{p-1-n} \cdot \left[\frac{d^{n+1} \log(a_i + e^v a_j)}{dv^{n+1}} \right]_{v=0} \equiv 0 \pmod{p} \tag{2}$$

for $n = 1, 2, \ldots, p-2$, where B_n is the nth Bernoulli number and i, j are two of the three indices $1, 2, 3$.

In 1934, Krasner [2] used the criteria in (2) to show that if (1)p has solutions, where $p > (45!)^{88}$, then $B_{p-1-n} \equiv 0 \pmod{p}$ for $n = 1, 2, \ldots, 2[(\log p)^{1/3}]$. Recently Keller and Löh [1] have eliminated the condition $p > (45!)^{88}$ and Sami [5] has improved the upper bound to $[(\log p)^{2/5}]$. In this note, with a slight adaptation of Krasner's method, we prove the following:

THEOREM: If the First Case of Fermat's Last Theorem is false for prime p then p divides the numerator of B_{p-1-n} for $n = 1, 2, \ldots, [(\log p/\log\log p)^{1/2}]$.

In fact this theorem gives extremely strong heuristic evidence for supposing that the First Case of Fermat's Last Theorem is true. For, if one admits that the probability of p dividing B_{2n} is $1/p$, then the probability that $B_{p-1-2n} \equiv 0 \pmod p$, for each $2n \leq [(\log p/\log\log p)^{1/2}]$ is approximately $\exp(-(\log p)^{3/2}/2(\log\log p)^{1/2})$.

Lehmer [3] has shown that (1)p has no solutions for $p < 6.10^9$, so that the expected number of primes for which (1)p has solutions is less than 10^{-13}!

Although such heuristic evidence is not valid proof, it is interesting to note that Wagstaff's computations of B_n, for $n \leq 125{,}000$ (see [6]), conform well with our assumption.

We now proceed to the proof of the theorem.

Let $\Phi_n(X) = \sum_{k=1}^{n} \sum_{j=1}^{k} (-1)^j \binom{k-1}{j-1} j^{n-1} X^k$ for each $n \geq 1$ and R_n be the resultant of $\Phi_n(X)/X(1-X)$ and $X^n\Phi_n(X^{-1})/(1-X)$.

Krasner showed, for each $n \geq 1$, that

$$\Phi_n(t) = -\left[\frac{d^n \log(a_i+e^v a_j)}{dv^n}\right]_{v=0} \quad \text{where} \quad t = a_j/(a_i+a_j) \tag{3}$$

Furthermore that

$$0 < |R_n| < (n-1)!^{2(n-2)} \tag{4}$$

So suppose that (1)p has integer solutions a_1, a_2, a_3 for some prime $p > 6.10^9$, and that $B_{p-1-n} \not\equiv 0 \pmod p$ for some $n \leq (\log p/\log\log p)^{1/2}$.

Let t be the minimum positive residue of $a_2/(a_1+a_2) \pmod p$. Then $t \not\equiv 0$ or $1 \pmod p$, or else p divides $a_1a_2a_3$. Also, as $a_1+a_2+a_3 \equiv 0 \pmod p$, $t^{-1} \equiv a_3/(a_1+a_3) \pmod p$.

Thus, by (2) and (3), $\Phi_{n+1}(t) \equiv \Phi_{n+1}(t^{-1}) \equiv 0 \pmod p$; and so p divides R_{n+1}.

Now, by Stirling's formula, $n! < (n/e)^n(2\pi n)^{1/2}e^{1/12n}$ for each $n \geq 1$. Thus, as $R_{n+1} \neq 0$,

$$\log p \leq \log |R_{n+1}|$$

$$< 2(n-1)\log n! \qquad \text{by (4)}$$

$$< (n-1)[(2n+1)\log n - 2n + \log 2\pi + 1/6n]$$

$$< 2n^2 \log n \qquad \text{for } n \geq 2$$

$$\leq 2 \cdot \frac{\log p}{\log\log p} \cdot \frac{1}{2}(\log\log p - \log\log\log p)$$

$$< \log p \quad \text{which establishes a contradiction.}$$

Thus $B_{p-1-n} \equiv 0 \pmod p$ for each $n \leq (\log p/\log\log p)^{1/2}$.

References

[1] W. KELLER and G. LÖH, The Criteria of Kummer and Mirimanoff extended to include 22 Consecutive Irregular Pairs, Tokyo J. Math., 6, (1983), 397-402

[2] M. KRASNER, Sur le premier cas du théorème de Fermat, C. R. Acad. Sci. Paris, 199, (1934), 256-258

[3] D. H. LEHMER, On Fermat's quotient, base two, Math. Comp., 36 (1981), 289-290

[4] P. RIBENBOIM, 13 Lectures on Fermat's Last Theorem, Springer, New York - Heidelberg - Berlin, 1979

[5] Z. SAMI, On the first case of Fermat's Last Theorem, to appear in Glasnik Matematicki, 21 (1986)

[6] S. S. WAGSTAFF, JR., The irregular primes to 125,000, Math. Comp. 32, (1978), 583-591

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

(Received March 11, 1986)