COLLOQUIUM MATHEMATICUM

VOL. LXVII 1994 FASC. 1

ON KRASNÉR'S THEOREM FOR THE FIRST CASE OF FERMAT'S LAST THEOREM

BY

VIJAY JHA (ALLAHABAD)

1. Introduction. In 1934 Krasnér [3] deduced from Kummer's congruences for the first case of Fermat's Last Theorem (abbreviated FLT1) that if FLT1 fails for the prime p, and the Bernoulli number $B_{p-n-1} \not\equiv 0 \pmod p$ for even $n, 2 \le n \le p-3$, then

$$\log p < f(n) \quad \text{where} \quad f(n) = 2(n-1)\log(n!). \tag{1}$$

From this he derived that for $n < k(p) = 2(\log p)^{1/3}$ and $p > (45!)^{88}$, $B_{p-1-n} \equiv 0 \pmod p$. The restriction $p > (45!)^{88}$ was removed later by Wada [5] and Keller and Löh [2].

In 1986 Sami [4], by transforming Kummer's congruences, obtained the bound $S(p) = (\log p)^{0.4}$. Later Granville [1] used (1) to obtain the bound $G(p) = ((\log p)/\log\log p)^{1/2}$.

In Section 2 we show that, without going through the lengthy transformations of Sami, a slightly better bound with exponent $0.4057\ldots$ can be directly obtained from (1). In fact, in the following proposition we give a more definite result.

1.1. PROPOSITION. *Let $h(n) = (\log(f(n)))/(\log n)$. Then the best possible bound implied by* (1) *and of the type $(\log p)^c$ is attained for $c = 1/h(22) = 0.405761\ldots$*

Next we ask the question: "what is the best possible bound, resulting from (1) and without any restriction on the type?". Here, the exact bound may be complicated, so we raise the question of asymptotically best bound. Throughout we say $\phi \approx \varphi$ if both are defined and nonzero in an interval $x > x_0$ and

$$\lim_{x\to\infty} \phi(x)/\varphi(x) = 1.$$

1991 *Mathematics Subject Classification*: Primary 11D41, 11B68.

This work is part of the author's Ph.D. thesis submitted to the Panjab University, Chandigarh, India.

A bound $h_1(p)$ is called *asymptotically best* if for any other bound $h_2(p) \geq h_1(p), h_1(p) \approx h_2(p)$. In Section 2 we prove

1.2. PROPOSITION. *Let $\vartheta(p)$ be a bound resulting from* (1) *and such that $\vartheta(p) \geq G(p)$. Then $\lim_{p\to\infty} \vartheta(p)/G(p) = 1$.*

It follows that Granville's bound is asymptotically the best possible solution of Krasnér's inequality (1), and by this method one cannot expect any further improvements. Thus for any essential improvement one has to modify Krasnér's method at an early stage and try to improve the inequality (1). In Section 3 we accomplish this by factoring the resultant into smaller integers. Precisely, we prove

1.3. THEOREM. *Let the first case of Fermat's Last Theorem fail for an odd prime p and let*

$$V(p) = \max\{(2(\log p)/\log\log p)^{1/2}, (\log p)^{617/1398}\}.$$

Then $B_{p-1-n} \equiv 0 \pmod p$ for $1 < n \leq V(p)$.

1.4. Remark. It follows that the bound $V(p)$ is better than the bounds $S(p)$ and $G(p)$ and that it cannot be obtained by the methods of Krasnér, Sami and Granville. *Although we improve over Granville only by a constant factor, it needs a basically new idea.*

2. Proofs of Propositions 1.1 and 1.2. Let $n!$ denote the value of the Gamma function of a real variable at $n+1$. Then the function of real variable $f(n) = 2(n-1)\log(n!)$ strictly increases for $n > 1$. Let f^{-1} denote the inverse function. Then (1) is equivalent to the inequality $f^{-1}(\log p) < n$.

2.1. Proof of Proposition 1.1. We are looking for the best (i.e. largest) c such that for $n \leq (\log p)^c, B_{p-1-n} \equiv 0 \pmod p$. By the result of Krasnér quoted at the beginning, this would certainly be the case if $n \leq (\log p)^c$ implies that $f(n) \leq \log p$, i.e., if $f(n) \leq n^{1/c}$. Now, $f(n) < n^u$ if and only if $h(n) \leq u$ where $h(n) = (\log(f(n)))/(\log n)$. Thus the best u is $\max\{h(n) : n \in \mathbb{Z}^+\}$.

Direct computation for integers $n < 150$ yields that the maximum of $h(n)$ for integers in this interval is attained for $n = 22$. We now show that $h(n) \leq h(22)$ for all $n \in \mathbb{Z}^+$. Obviously

$$f(n) < 2n^2 \log n \tag{2}$$

and hence

$$h(n) < 2 + (\log(2(\log n)))/(\log n).$$

The right hand side of the above, as a function of real variable, strictly decreases for $n > 5$ and since it is less than $h(22)$ at $n = 150$, it must be so for $n > 150$. ∎

Remark. The above result contains Sami's [4] result and decides the problem in a more definite way.

2.2. Proof of Proposition 1.2. We first notice that the best possible bound is obviously $f^{-1}(\log p)$. Let $H(x) = (x/(\log x))^{1/2}$. It is enough to show that $f^{-1}(\log p) \approx G(p)$, where $G(p) = H(\log p)$ is Granville's bound. For this, it would be sufficient to show that $f^{-1}(x) \approx H(x)$. Let now $g(x) = 2x^2(\log x)$. Then

$$\lim_{x\to\infty} g^{-1}(x)/H(x) = \lim_{y\to\infty} g^{-1}(g(y))/H(g(y)) = \lim_{y\to\infty} y/H(g(y)).$$

Since

$$H(g(y)) = y(2(\log y)/(\log 2 + 2(\log y) + \log\log y))^{1/2},$$

it follows that $g^{-1}(x) \approx H(x)$. To prove the proposition, it is sufficient to show that $f^{-1} \approx g^{-1}$. Since both are strictly increasing and the derivative g' also increases, the proposition follows from the following lemma.

2.3. Lemma. *Let the functions f and g be strictly increasing, continuous, unbounded for $x > x_0$ and $f \approx g$. Suppose that $f < g$ for $x > x_0$ and g has continuous derivative which is a nondecreasing function of x in some neighborhood of infinity. Then $f^{-1} \approx g^{-1}$.*

Proof. Let $\varepsilon > 0$. As $f \approx g$, there exists $x_1 > 0$ such that $\forall x > x_1$, $f(x) < g(x) < (1+\varepsilon)f(x)$. Put $g^{-1} = \phi$. Then

$$\forall x > x_1, \quad \phi(f(x)) < x < \phi((1+\varepsilon)f(x)),$$

or $1 < x/\phi(f(x)) < 1 + \varepsilon L(x)$, where

$$L(x) = (\phi((1+\varepsilon)f(x)) - \phi(f(x)))/(\varepsilon\phi(f(x))).$$

Now, by the Mean Value Theorem,

$$L(x) = f(x)\phi'((1+\delta)f(x))/\phi(f(x)) \quad \text{for some } \delta,\ 0 < \delta < \varepsilon.$$

As $\phi'(z) = 1/g'(\phi(z))$, and g' is nondecreasing, $g'(z) \le g'((1+\delta)z)$. Therefore $L(x) \le g(y)/(yg'(y))$ for $y = \phi(f(x))$. But this implies that if $y_1 = \phi(f(x_1))$ then

$$\begin{aligned} L(x) &\le g(y_1)/(yg'(y)) + (g(y) - g(y_1))/(yg'(y)) \\ &\le g(y_1)/(yg'(y)) + (y - y_1)g'(z)/(yg'(y)) \end{aligned}$$

for some z, $y_1 < z < y$. Thus, there exist x_2 such that $L(x) < 2$ for all $x > x_2$. Hence, $1 < x/\phi(f(x)) < 1 + 2\varepsilon$ for all sufficiently large x. ∎

3. Proof of Theorem 1.3. The proof consists of several steps. First we state some known facts and notation. Let the first case fail for the prime p. Then there exist integers x, y, z, such that

$$x^p + y^p + z^p = 0, \quad p \nmid xyz. \tag{3}$$

Let the polynomials M_i be defined as follows:

$$M_1 = -T, \quad M_{i+1}(T) = T(1-T)M_i'(T) \quad \text{for } i \geq 1. \tag{4}$$

Then Krasnér [3] showed that for $t = y/(x+y)$,

$$\frac{d^i \log(x + ye^v)}{dv^i}\Big|_{v=0} = -M_i(t), \tag{5}$$

and deduced that if in addition $B_{p-i} \not\equiv 0 \pmod p$, then the nonzero resultant R_i of $M_i(T)/T(1-T)$ and $T^i M_i(1/T)/(1-T)$ vanishes modulo p. First we summarize some known properties of M_i.

3.1. Lemma (see [3]). *Let $i \geq 1$. Then the leading coefficient of $M_i(T)$ is $(-1)^i(i-1)!$ and the coefficient of T is -1. The roots of M_i are real, simple and lie in the closed unit interval $[0,1]$.*

3.2. Lemma. *Let $i \geq 3$ be odd. Then $M_i(T) = T(1-T)(2T-1)N_i(T)$, where N_i is of degree $d = i-3$ and has integer coefficients. Further,*

$$N_i(1-T) = N_i(T), \tag{6}$$

and if $N_i^*(T) = T^{i-3}N_i(1/T)$ then N_i^* is monic with integer coefficients and constant term $A = (i-1)!/2$.

Proof. First we show by induction upon i that for $i \geq 2, M_i(1-T) = (-1)^i M_i(T)$. This is obvious for $i = 2$. Let it be true for i. By differentiating the identity $M_i(1-T) = (-1)^i M_i(T)$ and multiplying by $T(1-T)$ we deduce from (4) that $M_{i+1}(1-T) = (-1)^{i+1}M_{i+1}(T)$. The assertion follows.

Next, for odd $i \geq 3, M_i(1/2) = -M_i(1/2)$ and thus $M_i(1/2) = 0$. Hence $2T-1$ divides $M_i(T)$, so $M_i = T(1-T)(2T-1)N_i$ where $N_i \in \mathbb{Z}[T]$. The remaining assertions follow from the above and Lemma 3.1. ∎

In the next lemma we factor the resultant S_i of N_i and N_i^* (by Lemmas 3.1 and 3.2 it is obvious that $S_i \neq 0$). We assume that i is a fixed odd integer > 3 and $d = i-3$ is the degree of N_i.

3.3. Lemma. *Let $t_1 < \ldots < t_d$ be all the roots of N_i and let $t_k' = 1 - t_k$, $a_k = 1/t_k'$, $1 \leq k \leq d$. Put*

$$B = \prod_{j<k}(a_j a_k - 1), \qquad c = \prod_{k=1}^{d/2}(a_k/t_k - 1).$$

Then B and c are positive rational integers and c divides B. Let further S_i be the resultant of N_i and N_i^*. Then

$$S_i = N_i(1)N_i(-1)(bc)^2 \quad \textit{where} \quad b = B/c. \tag{7}$$

Proof. It is clear that B and c are positive. By Lemma 3.2, $1/t_k$ are roots of N_i^* and thus are algebraic integers. Since t_k are the roots of N_i, therefore again by Lemma 3.2, $1 - t_k$ are also roots of N_i and thus

$a_k = 1/(1-t_k)$ is an algebraic integer. It follows that B and c are algebraic integers. Since B is invariant under every permutation of the roots of $N_i^*(T)$, it must be a rational integer.

Further, let σ be any automorphism of the algebraic closure of the field of rationals. Then σ permutes the roots of every polynomial with rational coefficients. As $\sigma(t_j') = 1 - \sigma(t_j)$, for $t_j < 1/2$ either $\sigma(t_j) = t_k$ or $\sigma(t_j) = 1 - \sigma(t_k)$ for some $k < d/2$ (we use the obvious fact that by (6) half of the roots of N_i are less than $1/2$ and the other half are $> 1/2$). Thus σ leaves c unchanged and hence c is also a rational integer. Next, $S_i = \prod_{j,k=1}^{d}(a_k a_j - 1) = uv$, where

$$u = \prod_{k=1}^{d}(a_k^2 - 1) = N_i(1)N_i(-1), \qquad v = \prod_{j\neq k}(a_k a_j - 1) = B^2.$$

Finally, for $1 < k < d/2, a_k = a_j$ for some $j > d/2$ and thus $a_k/t_k = a_j a_k$. This shows that c divides B. ∎

3.4. Lemma. *Let $d > 6$ and $W(d) = A^{d-2}(3/4)^{d(d-2)/2}$. Then the integers $N_i(1), N_i(-1)$, c and b are positive and less than $W(d)$. Further,*

$$\log(W(d)) < (d+2)^{1398/617}.$$

Proof. Let $u_{jk} = (1-t_jt_k)(1-t_jt_k')(1-t_j't_k)(1-t_k't_j')$. Then

$$S_i = A^{2d}\prod_{j,k=1}^{d}(1-t_kt_j) = \Big\{A^{d-2}\prod_{j<k}^{d/2}u_{jk}\Big\}^2 A^4\prod_{j=1}^{d/2}u_{jj}.$$

However,

$$\begin{aligned} A^4\prod_{j=1}^{d/2}u_{jj} &= A^4\prod_{j=1}^{d/2}(1-t_j^2)(1-t_j'^2)(1-t_jt_j')^2 \\ &= \Big\{A^2\prod_{j=1}^{d/2}(1-t_j^2)(1-t_j'^2)\Big\}\Big\{A\prod_{j=1}^{d/2}(1-t_jt_j'^2)\Big\}^2 = N_i(1)N_i(-1)c^2. \end{aligned}$$

Hence, by (7),

$$b = A^{d-2}\prod_{j<k}^{d/2}u_{jk}. \tag{8}$$

Now $u_{jk}^{1/4}$, as the geometric mean of four numbers, must be less than their arithmetic mean, which turns out to be $3/4$. Thus $u_{jk} < (3/4)^4$ and (8) gives $b < A^{(d-2)}(3/4)^{d(d-2)/2}$. This implies that $b < W(d)$.

Further, $\max\{c, N_i(1)\} < A < N_i(-1)$ and

$$N_i(-1) = A\prod_{k=1}^{d}(1+t_k) = A\prod_{k=1}^{d/2}(1+t_k)(1+t'_k).$$

Since for $0 < x < 1/2, (1+x)(2-x) < 9/4$ and $1+t'_k = 2-t_k$, we get $N_i(-1) < A(3/2)^d$. As $A = (i-1)!/2 = (d+2)!/2$ (see Lemma 3.2), it follows that for $d > 6, A(3/2)^d < W(d)$.

To get the bound for $W(d)$, let $n = d+2$. By Stirling's formula,

$$n! < (2\pi e)^{1/2} e^{1/(12n)} (n/e)^{n+0.5}.$$

Let $X_n = \log\{(\pi e/2)^{.5} e^{1/(12n)} (n/e)^{n+.5} (3/4)^{n/2-1}\}$. Then

$$\log(W(d)) < (n-4)X_n.$$

Now $\log\{(\pi e/2)^{0.5} e^{1/(12n)} (3/4)^{n/2-1}\} < 0$, for $n \geq 8$, and thus

$$\log(W(d)) < n^2 \log(n/e) \quad \text{for } n \geq 8. \tag{9}$$

Let $u = 164/617$. Now the function $\alpha(m) = -um + \log(m-1)$ defined for real $m > 1$ has a unique maximum at $m = 1 + 1/u$. Also $\exp(\alpha(\log n)) = (n^{-u} \log(n/e))$. It follows that $\alpha(\log n) < 0$ if and only if $n^2 \log(n/e) < n^{2+u}$ and in this case $\log(W(d)) < n^{2+u}$. Let $x_0 = e^{1+1/u}$. It can be verified that for $x_1 = 500, \alpha(\log x_1) < 0$. Since $x_1 > x_0$ and α decreases for $x > \log x_0$, we get $\log(W(d)) < n^{2+u}$ for $n > 500$. If $6 \leq n < 500$, then it can be verified computationally that $\log(W(d)) < (n-4)X_n < n^{2+u}$. ∎

3.5. Proof of the Theorem. Let FLT1 fail for the prime $p > 2$ and suppose that $B_{p-1-n} \not\equiv 0 \pmod p$ for $2 \leq n \leq p-3$. Then by [2], $n \geq 44$. Let $t = y/(x+y)$. In the first case $t \not\equiv 0, 1 \pmod p$. Krasnér [3] showed that in this case $M_{n+1}(t)$ and $M_{n+1}(1/t)$ both vanish modulo p.

If $t \equiv 1/2 \pmod p$ then, as $x+y+z \equiv 0 \pmod p$, we get $x \equiv y \pmod p$ and hence $y/(y+z) \equiv -1 \pmod p$. Replacing x by z, we get $N_{n+1}(-1) \equiv 0 \pmod p$. By Lemma 3.4, $p < N_{n+1}(-1) < W(n-2)$.

If $t \not\equiv 1/2 \pmod p$ then by Lemma 3.2, t is the common root of N_{n+1} and N^*_{n+1} modulo p and thus their resultant $S_{n+1} \equiv 0 \pmod p$. By Lemma 3.3, p must divide one of the integers $N_{n+1}(1), b, c$ and $N_{n+1}(-1)$. By Lemma 3.4 once more $p < W(n-2)$.

Thus in every case $p < W(n-2)$. By Lemma 3.4, $\log p < n^{1398/617}$ or $n > (\log p)^{617/1398}$. Using (9) we obtain $\log p < n^2 \log(n/e)$. Since the value of the increasing function $\alpha^2 \log(\alpha/e)$ at $\alpha = (2(\log p)/\log\log p)^{1/2}$ is less than $\log p$, we conclude that $n \geq (2(\log p)/\log\log p)^{1/2}$. Hence $n \geq V(p)$. ∎

3.6. Remark. It is known [5] that the set $H = \{x/y, y/x, x/z, z/x, y/z, z/y\}$, considered modulo p, can have 2, 3 or 6 elements. The factorization of the resultant conducted in Lemma 3.3 shows that the factor b (needing the largest majorant) must correspond to the case when H has 6 elements.

As reported in [2], [5], in this case (for $n \leq 44$) by using other roots and solving the simultaneous polynomial system of congruences [5], the possible primes p come out to be much smaller than $N_i(-1)$. If this could be proved for all n then we would (by using the bound for $N_i(-1)$ obtained in Lemma 3.4) have the following result.

3.7. CONJECTURE. *If* FLT1 *fails for the prime* p *then* $B_{p-1-n} \equiv 0 \pmod{p}$ *for* $1 \leq n \leq (\log p)/(\log\log p)$.

REFERENCES

[1] A. Granville, *On Krasnér's criteria for the first case of Fermat's Last Theorem*, Manuscripta Math. 56 (1987), 67–70.
[2] 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.
[3] M. Krasnér, *Sur le premier cas du théorème de Fermat*, C. R. Acad. Sci. Paris 199 (1934), 256–258.
[4] Z. Sami, *On the first case of Fermat's Last Theorem*, Glas. Mat. 21 (1986), 295–296.
[5] H. Wada, *Some computations on the criteria of Kummer*, Tokyo J. Math. 3 (1980), 173–176.

MEHTA RESEARCH INSTITUTE OF MATHEMATICS
10, KASTURBA GANDHI MARG
OLD KUTCHERY ROAD
ALLAHABAD 211002, INDIA

Reçu par la Rédaction le 3.1.1992;
en version modifiée le 11.8.1993