TOKYO J. MATH.
VOL. 6, NO. 2, 1983

The Criteria of Kummer and Mirimanoff Extended to Include 22 Consecutive Irregular Pairs

Wilfrid KELLER and Günter LÖH

University of Hamburg

(Communicated by Y. Kawada)

Introduction

Let p be an odd prime and r an integer with $1 \leqq r \leqq (p-3)/2$. If p divides the numerator of the Bernoulli number $B_{p-(2r+1)}$, or, equivalently, if $B_{p-(2r+1)} \equiv 0 \pmod{p}$, then the pair $(p, p-(2r+1))$ is said to be an irregular pair. For a given prime p, irregular pairs corresponding to consecutive integers r are called consecutive irregular pairs. The existence of consecutive irregular pairs associated with a prime p is intimately connected with the possibility of finding a nontrivial solution to the Fermat equation $x^p+y^p+z^p=0$ for the case that $(xyz, p)=1$. Thus, Wada [9] proved in 1979:

PROPOSITION 1. *If* $x^p+y^p+z^p=0$ *and* $(xyz, p)=1$, *then* $B_{p-(2r+1)} \equiv 0 \pmod{p}$ *for* $r=1, 2, \cdots, 9$.

This proposition generalizes earlier results of Kummer (1857) and Mirimanoff (1905). For a history of the problem, see [8]. The condition imposed for a solution x, y, z to exist is a very stringent one. Since looking at all irregular pairs for primes $p<125000$ [10] and $1 \leqq r \leqq 9$, not even two consecutive pairs are found, nor a single pair appears for $r=3$ or $r=6$. The following result, which, for sufficiently large values of p, is stronger than Wada's, was proved by Krasner [2] in 1934:

PROPOSITION 2. *If* $x^p+y^p+z^p=0$ *and* $(xyz, p)=1$, *and if* $p>n_0=(45!)^{88}$, *then* $B_{p-(2r+1)} \equiv 0 \pmod{p}$ *for* $r=1, 2, \cdots, k(p)$, *where* $k(p)=[\sqrt[3]{\log p}]$.

Note that the assumption of $p>n_0$ implies $k(p) \geqq [\sqrt[3]{\log n_0}]=22$. From Propositions 1 and 2 a number of summation criteria may be derived using the following result, proved by Ribenboim [7] in 1978:

Received July 15, 1982

PROPOSITION 3. *If* $B_{p-(2r+1)} \equiv 0 \pmod{p}$, *with* $1 \leqq r \leqq (p-3)/2$, *then*

$$\sum_{j=1}^{[p/8]} \frac{1}{j^{2r+1}} \equiv 0 \pmod{p} \quad \textit{and} \quad \sum_{j=1}^{[p/6]} \frac{1}{j^{2r+1}} \equiv 0 \pmod{p} .$$

In this paper, Proposition 1 is extended to include 22 irregular pairs. That result, combined with Proposition 2, yields an enlarged set of summation criteria based on Proposition 3.

§1. The results.

Taking advantage of the method developed by Wada [9], Proposition 1 could be extended by merely carrying out some rather complicated numerical computations summarized in the next section. So we obtained

PROPOSITION 4. *If* $x^p+y^p+z^p=0$ *and* $(xyz, p)=1$, *then* $B_{p-(2r+1)} \equiv 0 \pmod{p}$ *for* $r=1, 2, \cdots, 22$.

TABLE 1

All primes $p_r \geqq 3$, $q_r \geqq 7$, p_r, $q_r < 30000$, satisfying $\sum_{j=1}^{[p_r/3]} \frac{1}{j^{2r+1}} \equiv 0 \pmod{p_r}$, $\sum_{j=1}^{[q_r/6]} \frac{1}{j^{2r+1}} \equiv 0 \pmod{q_r}$

r	Values of p_r	Values of q_r
0	11	61
1	16843	16843
2	37	37
3	13	661
4	41, 67, 877	67, 149, 877
5	11, 61, 9311	9311
6	73	29, 3299
7	59, 547, 607 1093,	59, 457, 541, 607, 2113
8	41, 193, 2591	23, 2591
9	13, 37, 149, 311, 401, 757, 10133	149, 311, 401, 10133
10	11, 61, 1181, 8369	8369
11	67, 661, 3851	97, 2039, 2153
12	41, 73, 6481	53
13		
14	547, 1093, 4219, 9133, 16493	4219, 9133
15	11, 13, 61, 271, 3323, 4561	41, 3323
16	41, 101, 193, 2267	101, 2267
17	103, 307, 1021, 1871	569
18	73, 757	73, 149
19	1597, 2851, 3181, 3529	23, 719, 3181, 3529
20	11, 37, 61, 773, 1181	29, 37, 239, 773, 4871
21	13, 547, 1093, 2269	173
22	67, 661, 3851, 5501	257, 19163

This result is combined with Proposition 2 to give the following, which no longer explicitly contains the constant n_0:

PROPOSITION 5. *If* $x^p+y^p+z^p=0$ *and* $(xyz, p)=1$, *then* $B_{p-(2r+1)}\equiv 0 \pmod p$ *for* $r=1, 2, \cdots, k(p)$, *where* $k(p)=\max(22, [\sqrt[3]{\log p}])$.

Following Ribenboim [7], we may conclude from this and Proposition 3:

PROPOSITION 6. *If* $x^p+y^p+z^p=0$ *and* $(xyz, p)=1$, *then*

$$\sum_{j=1}^{[p/3]} \frac{1}{j^{2r+1}} \equiv 0 \pmod p \quad \text{and} \quad \sum_{j=1}^{[p/6]} \frac{1}{j^{2r+1}} \equiv 0 \pmod p$$

for $r=1, 2, \cdots, k(p)$, *where* $k(p)=\max(22, [\sqrt[3]{\log p}])$.

TABLE 2

Factorizations for extending the criteria of Kummer and Mirimanoff on the basis of Wada's general proof

None of the prime factors p below satisfies $2^{p-1}\equiv 1 \pmod{p^2}$

$Q_{21}(-2)=5\cdot 11\cdot 37\cdot 229\cdot 21816493\cdot 87791779$

$Q_{23}(-2)=23\cdot 37316585794249136007887$

$Q_{25}(-2)=5^3\cdot 7\cdot 13\cdot 39276810737\cdot 2207141985991$

$Q_{27}(-2)=31\cdot 149\cdot 2969\cdot 6414013\cdot 15166743168064927$

$Q_{29}(-2)=5\cdot 29\cdot 37\cdot 680969383\cdot 574584477448029739651$

$Q_{31}(-2)=7\cdot 11\cdot 31\cdot 4289\cdot 85247\cdot 435543927052555022508 3101$

$Q_{33}(-2)=5\cdot 17\cdot 66643\cdot 13855009166921843518 67530069477303$

$Q_{35}(-2)=5804794024012902073\cdot 3157442156165383128206497$

$Q_{37}(-2)=5\cdot 7^2\cdot 13\cdot 19\cdot 37\cdot 449\cdot 36017\cdot 302985283\cdot 438128664354420273539 6813$

$Q_{39}(-2)=659\cdot 709\cdot 217661\cdot 5947555249\cdot 23058395306393\cdot 10085476072819643$

$Q_{41}(-2)=5\cdot 11\cdot 41\cdot 47\cdot 430928790848464941553882047243284227 1347380758713$

$Q_{43}(-2)=7\cdot 43\cdot 73\cdot 109\cdot 151\cdot 199\cdot 81839\cdot 277923933989654585803928386424762660553863$

$Q_{45}(-2)=5^2\cdot 23\cdot 112107458010167511347062945482008026510827970744623641753 03$

$S_{21}=-43\cdot 241\cdot 5419\cdot 9496386083$

$S_{23}=2796203\cdot 80348736972167$

$S_{25}=-7\cdot 11\cdot 13^2\cdot 251\cdot 4051\cdot 28447\cdot 300455201$

$S_{27}=19\cdot 3461\cdot 16759\cdot 87211\cdot 697446897311$

$S_{29}=-53\cdot 59\cdot 15083\cdot 3033169\cdot 7547263\cdot 42800473$

$S_{31}=7\cdot 31\cdot 715827883\cdot 236017358500033404991$

$S_{33}=-67\cdot 683\cdot 20857\cdot 36293\cdot 38177\cdot 25078104767246023$

$S_{35}=11\cdot 43\cdot 281\cdot 1249\cdot 86171\cdot 2371981599141956245883063$

$S_{37}=-7\cdot 13^3\cdot 19\cdot 37\cdot 1777\cdot 3343\cdot 18541\cdot 151871\cdot 25781083\cdot 8361790201$

$S_{39}=23\cdot 2731\cdot 22366891\cdot 3557857781106398296067286 2780147$

$S_{41}=-83\cdot 175427911\cdot 8831418697\cdot 552972895573825165951583191$

$S_{43}=7^2\cdot 43\cdot 2932031007403\cdot 180739851272443152096 8114002912181$

$S_{45}=-11\cdot 19\cdot 53\cdot 331\cdot 18837001\cdot 27892600130363017744369721226879745104 53$

$D_{21}=11$	$D_{23}=23$	$D_{25}=13$	$D_{27}=1$
$D_{29}=29\cdot 31$	$D_{31}=11\cdot 31$	$D_{33}=17$	$D_{35}=1$
$D_{37}=13\cdot 19\cdot 37$	$D_{39}=1$	$D_{41}=11\cdot 41$	$D_{43}=43$
$D_{45}=23$			

That proposition is known also to be true for $r=0$. In Table 1, we present all primes $p<30000$ satisfying any of these criteria for $0\leqq r\leqq 22$.

§2. The computations.

In order to prove Proposition 4 for a given value of r, three well-defined numbers $Q_{2r+1}(-2)$, S_{2r+1}, D_{2r+1} have to be computed. If the complete factorizations of these three numbers are established, and if none of the resulting prime factors p satisfies, say, the Wieferich

TABLE 3

Primality proofs for large factors of numbers $Q_{2r+1}(-2)$ and S_{2r+1}
$b(p)$ denotes the least positive primitive root
modulo a prime p

$p_1=Q_{31}(-2)/(7\cdot 11\cdot 31\cdot 4289\cdot 85247)$	
$p_2=Q_{33}(-2)/(5\cdot 17\cdot 66643)$	
$p_3=Q_{35}(-2)/5804794024012902073$	
$p_4=Q_{37}(-2)/(5\cdot 7^2\cdot 13\cdot 19\cdot 37\cdot 449\cdot 36017\cdot 302985283)$	
$p_5=Q_{41}(-2)/(5\cdot 11\cdot 41\cdot 47)$	
$p_6=Q_{43}(-2)/(7\cdot 43\cdot 73\cdot 109\cdot 151\cdot 199\cdot 81839)$	
$p_7=Q_{45}(-2)/(5^2\cdot 23)$	
$p_8=S_{35}/(11\cdot 43\cdot 281\cdot 1249\cdot 86171)$	
$p_9=S_{39}/(23\cdot 2731\cdot 22366891)$	
$p_{10}=S_{41}/(-83\cdot 175427911\cdot 8831418697)$	
$p_{11}=S_{43}/(7^2\cdot 43\cdot 2932031007403)$	
$p_{12}=S_{45}/(-11\cdot 19\cdot 53\cdot 331\cdot 18837001)$	
$p_1-1=2^2\cdot 5^2\cdot 7\cdot 1553\cdot 7299367\cdot 548879823983$	$b(p_1)=2$
$p_2-1=2\cdot 3^2\cdot q_1$	$b(p_2)=3$
$q_1-1=2\cdot 7\cdot 11\cdot 3581\cdot q_2$	$b(q_1)=6$
$q_2-1=2^3\cdot 7\cdot 47\cdot 349\cdot 757\cdot 7673\cdot 4423249\cdot 5914193$	$b(q_2)=5$
$p_3-1=2^5\cdot 3\cdot 739\cdot 26699983\cdot 1666896930323$	$b(p_3)=5$
$p_4-1=2^2\cdot 11\cdot 4157\cdot 4645465651\cdot 5156318239$	$b(p_4)=2$
$p_5-1=2^3\cdot 3\cdot 191\cdot 10193\cdot 400678544537\cdot q_3$	$b(p_5)=5$
$q_3-1=2\cdot 31\cdot 83\cdot 1831\cdot 2477\cdot 9862310177266341611$	$b(q_3)=2$
$p_6-1=2\cdot 59\cdot 12796909\cdot q_4$	$b(p_6)=5$
$q_4-1=2^2\cdot 3\cdot 5^2\cdot 89\cdot 25409\cdot 145517\cdot 185707\cdot 10039174844579$	$b(q_4)=2$
$p_7-1=2\cdot 7\cdot 11\cdot 311\cdot q_5$	$b(p_7)=7$
$q_5-1=2^3\cdot 47\cdot 2797\cdot 379649\cdot 130067797\cdot 9402530599817\cdot 479375996186428521031$	$b(q_5)=3$
$p_8-1=2\cdot 13\cdot 607493\cdot 14355083\cdot 10461428273$	$b(p_8)=5$
$p_9-1=2\cdot 5612196718781\cdot 3169755052598356333$	$b(p_9)=2$
$p_{10}-1=2\cdot 3^2\cdot 5\cdot 7\cdot 877734754879087565002513$	$b(p_{10})=3$
$p_{11}-1=2^2\cdot 3\cdot 5\cdot 7\cdot q_6$	$b(p_{11})=6$
$q_6-1=2^2\cdot 3\cdot 31\cdot 233\cdot 367073501\cdot 1352548151863295753$	$b(q_6)=7$
$p_{12}-1=2^2\cdot 7\cdot 11\cdot q_7$	$b(p_{12})=2$
$q_7-1=2^4\cdot 263077\cdot 3185144704697\cdot 675470292510306017$	$b(q_7)=3$

congruence $2^{p-1}\equiv 1 \pmod{p^2}$, then the proposition holds for that particular r. For the definition of the numbers involved and a general proof, we refer to the paper [9] of Wada, which appeared in this same journal.

In Table 2, we give the factorizations of $Q_{2r+1}(-2)$, S_{2r+1}, D_{2r+1} for $r=10, 11, \cdots, 22$. The primality of all factors p having at least 25 decimal digits may be verified using Table 3. Let $b(p)$ denote the least positive integer x such that $x^{p-1}\equiv 1 \pmod{p}$ and, for all prime divisors q of $p-1$, $x^{(p-1)/q}\not\equiv 1 \pmod{p}$. Then $b(p)$ is the least positive primitive root modulo the prime p. The primality proofs for remaining primes with less than 25 digits are supposed to be easily reproduced.

All of our computations have been done on a TELEFUNKEN TR 440 computer utilizing the Rational Arithmetic System [1], and the factorization algorithms implemented by the second-named author. These include the "$p-1$" and "rho" methods of Pollard [5], [6] as well as the continued fraction method of Morrison and Brillhart [3]. Computational details will be given in a separate report to be made available by the authors.

A final remark should be devoted to the numbers D_{2r+1}. It would be desirable to find a characterization of these numbers in order to render their laborious calculation unnecessary. As a first step in that direction, Müller [4] recently succeeded in proving that if $p>7$, $r\geqq 1$, and if $2r\equiv 0 \pmod{(p-1)}$, then $p|D_{2r+1}$. But, unfortunately, the converse is not true, since $31|D_{29}$.

ACKNOWLEDGEMENTS. We thank Helmut Müller for pointing out to us the paper of Wada, and for helpful discussions concerning the numbers D_{2r+1}. Thanks are also due to Hideo Wada, who encouraged us to complete the above computations and supplied valuable information.

References

[1] I. BÜCHEL und W. KELLER, Ein Programmsystem für Rationale Arithmetik: Einführung und Beispielsammlung, Bericht Nr. 8004, Rechenzentrum der Universität Hamburg, 1980.

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

[3] M. A. MORRISON and J. BRILLHART, A method of factoring and the factorization of F_7, Math. Comp., **29** (1975), 183-205.

[4] H. MÜLLER, On some congruences concerning the criteria of Kummer, in preparation.

[5] J. M. POLLARD, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc., **76** (1974), 521-528.

[6] J. M. POLLARD, A Monte Carlo method for factorization, BIT, **15** (1975), 331-334.

[7] P. RIBENBOIM, Some criteria for the first case of Fermat's last theorem, Tokyo J. Math., **1** (1978), 149–155.

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

[9] H. Wada, Some computations on the criteria of Kummer, Tokyo J. Math., **3** (1980), 173–176.

[10] S. S. WAGSTAFF, JR., The irregular primes to 125000, Math. Comp., **32** (1978), 583–591.

Present Address:
RECHENZENTRUM DER UNIVERSITÄT HAMBURG
ROTHENBAUMCHAUSSEE 81
2000 HAMBURG 13
FEDERAL REPUBLIC OF GERMANY