NOTES ON A CONJECTURE OF P. ERDÖS. I

SABURÔ UCHIYAMA and MASATAKA YORINAGA

Let a and b be rational integers with $1 \leqq a < b$ and G. C. D. $(a, b) = 1$. For any natural number n we denote by $f(n) = f(n\,;\, a,\, b)$ the number of those integers k lying in the interval $1 \leqq k < (\log n)/\log(b/a)$, for which $a^k n - b^k$ is a prime number. P. Erdös [1, 2, 3] has considered in some detail properties of the function $f(n)$ for $a = 1$, $b \geqq 2$; indeed, in the particular case of $a = 1$, $b = 2$, he has proved among other things that there is a constant $c > 0$ such that we have

$$f(n) > c \log\log n$$

for infinitely many n, and that there exists an infinite arithmetic progression consisting only of odd integers n for which $f(n) = 0$ (cf. [1]). And, he conjectures that there holds

$$(1) \qquad f(n) = f(n\,;\, 1,\, b) = o(\log n) \qquad (n \to \infty)$$

for any fixed $b \geqq 2$ (cf. [1, 2]); at the present stage of our knowledge, (1) seems difficult to prove (or disprove).

It is possible for some natural numbers n that all of the integers

$$n - 2^k \qquad (1 \leqq k < (\log n)/\log 2)$$

are prime ; in fact, $n = 4$, 7, 15, 21, 45, 75 and 105 are such numbers, and Erdös [1] observes the fact that in the interval

$$(2) \qquad 105 < n \leqq 203775 = 3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 19$$

there are no other integers n of that kind.

For brevity's sake we shall say that a natural number n has the property $P(a, b)$, if all of the integers

$$a^k n - b^k \qquad (1 \leqq k < (\log n)/\log(b/a))$$

are prime numbers. Thus, Erdös [1, 2, 3] conjectures that 105 is the largest integer which has the property $P(1, 2)$. Using an electronic computer IBM 7040, W. E. Mientka and R. C. Weitzenkamp [4] have extended the interval (2) of non-existence for n with the property $P(1, 2)$ to

$$(3) \qquad 105 < n \leqq 187347246779555$$
$$(= 3 \cdot 5 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 29^2 \cdot 37 \cdot 79 > 2^{44}).$$

We also have examined on a computer HITAC 20 the existence of positive integers with the property P (1, 2) and found that in the interval

$$105 < n \leqq 152246817378604933869885$$
$$(= 3\cdot5\cdot7\cdot11\cdot13\cdot19\cdot29\cdot37\cdot53\cdot59\cdot61\cdot67\cdot38916793 > 2^{77})$$

there are no such integers n, thus extending further the interval (3) of non-existence. See Example 1 below.

We shall be primarily concerned in what follows with natural numbers having the property $P(a, b)$ with $1 \leqq a < b$, G. C. D. $(a, b) = 1$. A plausible conjecture is that there are at most finitely many positive integers with the property $P(a, b)$, whatever the integers a, b may be.

Most of the numerical computations relevant to our present investigations have been, or will be, done by a FORTRAN programme on a computer HITAC 20 in the Department of Mathematics, Okayama University.

1. Some numerical results. Mientka and Weitzenkamp [4] have given a table of the number of natural numbers $n \leqq 20000$ having the property $P(1, b)$ for each b with $2 \leqq b \leqq 13$. However, our numerical experiment suggests that there must be errors in their table, apart from a possible misprint. In fact, the numerals we have found are inconsistent with those in the table of Mientka and Weitzenkamp, and the discrepancy will be seen thus.

Number of natural numbers $n \leqq 20000$ with $P(1, b)$, $2 \leqq b \leqq 13$

b	Mientka-Weitzenkamp's	ours	difference
2	9	7	2
3	23	20	3
4	81	77	4
5	63	58	5
6	240	234	6
7	159	152	7
8	110	102	8
9	280	251	29
10	383	373	10
11	265	254	11
12	351	339	12
13	385	372	13

Number of natural numbers $n \leqq x$ with P(1, b), $2 \leqq b \leqq 21$, for $x = 2^m$E4, $m = 0(1)10$

b \ x	1E4	2E4	4E4	8E4	16E4	32E4	64E4	128E4	256E4	512E4	1024E4	largest n found
2	7	7	7	7	7	7	7	7	7	7	7	105
3	20	20	20	20	20	20	20	20	20	20	20	1330
4	70	77	80	88	90	92	94	97	99	99	100	5833497
5	54	58	59	60	61	61	63	64	65	65	66	7726572
6	206	234	271	294	325	349	359	375	387	398	411	9620063
7	134	152	162	175	193	199	214	225	233	242	247	9487050
8	94	102	117	125	135	153	169	183	195	203	210	8531205
9	202	251	332	392	452	534	680	771	890	1049	1117	10166362
10	315	373	462	582	661	746	867	988	1029	1083	1177	9981153
11	190	254	315	405	547	639	766	967	1178	1353	1581	10219608
12	253	339	376	417	470	525	566	637	747	808	853	10203655
13	269	372	477	530	615	751	862	984	1169	1405	1511	10177200
14	221	308	438	536	696	921	1211	1405	1709	2177	2651	10238703
15	498	687	1002	1305	1610	2080	2796	3333	3852	4645	5972	10239754
16	430	568	803	1130	1389	1790	2358	3182	3709	4540	5929	10239467
17	196	241	303	396	435	474	525	621	659	708	773	10120650
18	385	474	598	802	980	1086	1247	1514	1823	2076	2473	10228645
19	411	525	696	999	1355	1580	1941	2482	3286	3547	4016	10230452
20	324	418	575	824	1213	1472	1886	2483	3448	4225	4933	10233093
21	679	916	1282	1830	2816	3717	4723	6320	8780	11949	14395	10237082

We have also tabulated for each b, $2 \leqq b \leqq 21$, the number of natural numbers $n \leqq x$ having the property $P(1, b)$ for $x = 2^m E\, 4$, $m = 0(1)10$, together with the largest n's so far found.

In a second Note under preparation we shall present some tables of the number of positive integers having the property $P(a, b)$ with $1 < a < b$, G. C. D. $(a, b) = 1$.

2. An exclusion procedure. Again, let, a, b be a pair of integers with $1 \leqq a < b$, G. C. D. $(a, b) = 1$. If a is odd, then one at most of the natural numbers n that have the property $P(a, b)$ satisfies

$$n \equiv 0 \pmod 2, \text{ or } n \equiv 1 \pmod 2$$

according as b is even, or is odd ; no such information is available if a is even and so b is odd. However, a much more effective exclusion processing can be achieved in general.

An odd prime q is called a *critical prime* for the pair of integers a, b, if G. C. D. $(q, ab) = 1$ and $\bar{a}b$ is a primitive root (mod q), where $\bar{a}$ is an integer (uniquely) detemined (mod q) by $\bar{a}a \equiv 1 \pmod q$. In particular, q is a critical prime for the pair 1, b if b itself is a primitive root (mod q). It seems likely that if there is a critical prime for a pair a, b, then there exist infinitely many critical primes for the pair a, b, though we cannot at present prove this fact rigorously.

Let $q_1, q_2, q_3, \cdots$ be if existent the increasing sequence of critical primes for the pair a, b. We define the quantities $Q_i = Q_i(a, b)$ $(i \geqq 1)$ and $M_i = M_i(a, b)$ $(i \geqq 1)$ by setting

$$Q_i = q_1 q_2 \cdots q_i$$

and

$$M_i = \max_{1 \leqq k \leqq q-1} \left[\frac{b^k + q}{a^k} \right]$$
$$= \max \left(\left[\frac{b + q}{a,} \right], \left[\frac{b^{q-1} + q}{a^{q-1}} \right] \right)$$

with $q = q_i$, where $[t]$ denotes the greatest integer not exceeding the real number t.

The notion of critical primes, when not meaningless, will be helpful for actual computations, as the following proposition shows.

Proposition. *Let q be a critical prime for the pair a, b. If a natural number n has the property $P(a, b)$ and if n is not divisible by*

q, then we have $n \leqq M_i$, where $q = q_i$. Hence, if n has the property $P(a, b)$ and $n > M_i$ for some $i \geqq 1$, then n is necessarily a multiple of Q_i.

Proof is immediate, since if n is not divisible by a critical prime q for the pair a, b, then we have for some k with $1 \leqq k \leqq q-1$

$$a^k n - b^k \equiv 0 \pmod{q}, \quad \text{or} \quad a^k n - b^k = q$$

when n has the property $P(a, b)$. Cf. [4 ; Corollary 2].

A simple consequence of the proposition is the

Corollary. *If $M_i < Q_{i-1}$ for some $i > 1$, then there are no natural numbers n with the property $P(a, b)$ in the interval $Q_{i-1} \leqq n < Q_i$.*

Thus, a (non-empty) set of critical primes will furnish an exclusion procedure.

Now, we shall give some examples of pairs of integers a, b admitting critical primes ; in each of these examples all critical primes less than 100 will be listed.

Example 1. $a = 1$, $b = 2$: $q_1 = 3$, $q_2 = 5$, $q_3 = 11$, $q_4 = 13$, $q_5 = 19$, $q_6 = 29$, $q_7 = 37$, $q_8 = 53$, $q_9 = 59$, $q_{10} = 61$, $q_{11} = 67$, $q_{12} = 83$.

i	Q_i	M_i
1	3	7
2	15	21
3	165	1035
4	2145	4109
5	40755	262163
6	1181895	268435485
7	43730115	68719476773
8	2317696095	4503599627370549
9	136744069605	288230376151711803
10	8341388245905	1152921504606847037
11	558873012475635	73786976294838206531
12	46386460035477705	4835703278458516698824787

Steps in processing the case of $a = 1$, $b = 2$

Step 1° Read data : control parameters C_i $(i = 1, 2, 3)$, test primes P_r $(1 \leqq r \leqq C_1)$, starting value of the number n, and the increment h.

Step 2° Compute 2^k $(1 \leqq k \leqq C_2)$.

Step 3° Compute $g_k = n - 2^k$ $(1 \leqq k < B_n = (\log n)/\log 2)$.

Step 4° Put $r = 1$.

Step 5° Put $k = 1$.

Step 6° Test divisibility by p_r of g_k.

Step 7° If $p_r \mid g_k$ and $p_r < g_k$, then go to Step 13°.

Step 8° Put $k = k + 1$.

Step 9° If $k < B_n$, then go to Step 6°.

Step 10° Put $r = r + 1$.

Step 11° If $r \leqq C_1$, then go to Step 5°.

Step 12° Print the message 'Further Test' and go to Step 14°.

Step 13° If $p_r \geqq C_3$, then print the result.

Step 14° Put $n = n + h$ and go to Step 3°.

In the actual performance, we split our computations into several stages, according to the magnitude of the current value of n and the size of h. As an underlying set of test primes, we prepared about 300 prime numbers in number, excluding the critical primes less than the one for each of the stages just concerned.

Surprisingly enough, we have observed that for each number n in the range we examined, $n - 2^k > 0$ was divisible for some integer k by a relatively small prime number ; indeed, such prime numbers did not go beyond the prime 179, which appeared only for

$$n = 626155561196942830203 15 \text{ and } 137764842721212074680455.$$

Example 2. $a = 1$, $b = 3$: $q_1 = 5$, $q_2 = 7$, $q_3 = 17$, $q_4 = 19$, $q_5 = 29$, $q_6 = 31$, $q_7 = 43$, $q_8 = 53$, $q_9 = 79$, $q_{10} = 89$.

i	Q_i	M_i
1	5	86
2	35	736
3	595	43046738
4	11305	387420508
5	350455	205891132094680

Example 3. $a = 1$, $b = 5$: $q_1 = 3$, $q_2 = 5$, $q_3 = 17$, $q_4 = 23$, $q_5 = 37$, $q_6 = 43$, $q_7 = 47$, $q_8 = 53$, $q_9 = 73$, $q_{10} = 83$, $q_{11} = 97$.

Example 4. $a = 1$, $b = 6$: $q_1 = 11$, $q_2 = 13$, $q_3 = 17$, $q_4 = 41$, $q_5 = 59$, $q_6 = 61$, $q_7 = 79$, $q_8 = 83$, $q_9 = 89$.

Example 5. $a = 1$, $b = 7$: $q_1 = 5$, $q_2 = 11$, $q_3 = 13$, $q_4 = 17$, $q_5 = 23$, $q_6 = 41$, $q_7 = 61$, $q_8 = 67$, $q_9 = 71$, $q_{10} = 79$, $q_{11} = 89$, $q_{12} = 97$.

Example 6. $a = 1$, $b = 8$: $q_1 = 3$, $q_2 = 5$, $q_3 = 11$, $q_4 = 29$, $q_5 = 53$, $q_6 = 59$, $q_7 = 83$.

Example 7. $a = 1$, $b = 10$: $q_1 = 7$, $q_2 = 17$, $q_3 = 19$, $q_4 = 23$, $q_5 = 29$, $q_6 = 47$, $q_7 = 59$, $q_8 = 61$, $q_9 = 97$.

Example 8. $a = 2$, $b = 3$: $q_1 = 7$, $q_2 = 11$, $q_3 = 17$, $q_4 = 31$, $q_5 = 37$, $q_6 = 41$, $q_7 = 59$, $q_8 = 83$, $q_9 = 89$.

i	Q_i	M_i
1	7	11
2	77	57
3	1309	656
4	40579	191751
5	1501423	2.184E6

The positive integers $n \leqq 512E4$ with P(2, 3) are: $n = 3$, 4, 5, 7, and 8.

Example 9. $a = 2$, $b = 5$: $q_1 = 11$, $q_2 = 17$, $q_3 = 23$, $q_4 = 47$, $q_5 = 59$, $q_6 = 73$.

i	Q_i	M_i
1	11	9536
2	187	2328307
3	4301	5.684E8
4	202147	2.019E18
5	11926673	1.203E23

There are 34 positive integers $n \leqq 512E4$ with P(2, 5); the largest n found is : $n = 507$.

Example 10. $a=3$, $b=4$: $q_1=5$, $q_2=17$, $q_3=19$, $q_4=29$, $q_5=31$, $q_6=41$, $q_7=43$, $q_8=53$, $q_9=67$, $q_{10}=79$, $q_{11}=89$.

i	Q_i	M_i
1	5	3
2	85	99
3	1615	177
4	46835	3149
5	1451885	5599

The positive integers $n \leqq 512E4$ with P(3, 4) are: $n = 2$, 3, and 5.

Example 11. $a=3$, $b=5$: $q_1=13$, $q_2=23$, $q_3=29$, $q_4=31$, $q_5=41$, $q_6=47$, $q_7=73$, $q_8=79$, $q_9=83$, $q_{10}=89$.

i	Q_i	M_i
1	13	459
2	299	75975
3	8671	1.628E6
4	268801	4.523E6
5	11020841	7.480E8

The positive integers $n \leqq 512E4$ with P(3, 5) are: $n = 4$, 6, 12, and 24.

Example 12. $a=4$, $b=5$: $p_1=3$, $q_2=7$, $q_3=13$, $q_4=17$, $q_5=23$, $q_6=43$, $q_7=47$, $q_8=53$, $q_9=67$, $q_{10}=83$, $q_{11}=97$.

i	Q_i	M_i
1	3	2
2	21	3
3	273	14
4	4641	35
5	106743	135

$n = 2$ is the only positive integer with P(4, 5) less than $Q_{11} > 6.167\text{E}15$.

Example 13. $a=5$, $b=6$: $q_1=23$, $q_2=41$, $q_3=47$, $q_4=53$, $q_5=59$, $q_6=67$, $q_7=73$, $q_8=89$, $q_9=97$.

i	Q_i	M_i
1	23	55
2	943	1469
3	44321	4388
4	2349013	13104
5	138591767	39130

There are no positive integers with P(5, 6) less than $Q_9 > 5.851\text{E}15$.

Example 14. $a=6$, $b=7$: $q_1=5$, $q_2=23$, $q_3=37$, $q_4=59$, $q_5=67$, $q_6=71$, $q_7=73$, $q_8=83$, $q_9=97$.

i	Q_i	M_i
1	5	2
2	115	29
3	4255	257
4	251045	7636
5	16820015	26211

$n = 2$ is the only positive integer with P(6, 7) less than $Q_9 > 7.018\text{E}14$.

Example 15. $a=7$, $b=8$: $q_1=3$, $q_2=17$, $q_3=23$, $q_4=29$, $q_5=37$, $q_6=41$, $q_7=53$, $q_8=59$, $q_9=71$, $q_{10}=79$, $q_{11}=83$, $q_{12}=97$.

i	Q_i	M_i
1	3	1
2	51	8
3	1173	18
4	34017	42
5	1258629	122

There are no positive integers with P(7, 8) less than $Q_{12} > 7.286\text{E}18$.

Example 16. $a=7$, $b=9$: $q_1=5$, $q_2=11$, $q_3=17$, $q_4=23$, $q_5=41$, $q_6=61$, $q_7=71$, $q_8=89$, $q_9=97$.

i	Q_i	M_i
1	5	2
2	55	12
3	935	55
4	21505	251
5	881705	23215
6	53784005	3.537E6
7	3818664355	4.366E7
8	339861127595	4.024E9
9	32966529376715	3.005E10

$n = 2$ is the only positive integer with P(7, 9) less than $Q_4 = 21505$.

Example 17. $a=8$, $b=9$: $q_1=5$, $q_2=11$, $q_3=13$, $q_4=19$, $q_5=37$, $q_6=43$, $q_7=53$, $q_8=59$, $q_9=83$,

i	Q_i	M_i
1	5	1
2	55	3
3	715	4
4	13585	8
5	502645	69

There are no positive integers with P(8, 9) less than $Q_9 > 5.609\text{E}12$.

3. General observations. Let a, b be arbitrary integers satisfying $1 \leqq a < b$, G. C. D. $(a, b) = 1$. One may again conjecture that the function $f(n) = f(n; a, b)$ satisfies the relation (1) for every such pair of integers a, b.

Here, we mention two results on $f(n)$: the first of them is an extension, whereas the second is a weak generalization, of the results due to Erdös [1] quoted in the Introdnction.

Theorem 1. *We have*

$$\limsup_{n \to \infty} \frac{f(n; a, b)}{\log \log n} \geqq c$$

for some constant $c = c(a, b) > 0$.

In order to prove this theorem we apply, in place of a theorem of K. A. Rodosskiĭ[1] to which Erdös [1] appealed for the proof of his corresponding result with $a = 1$, $b = 2$, the Bombieri-Vinogradov mean value theorem on the remainder term in the prime number theorem for arithmetic progressions. As a result we find

$$c = \begin{cases} e^C \dfrac{\phi(b)}{b \log b} & \text{if } a = 1 \\ e^C \dfrac{\phi(b)}{b \log a} \log\left(\dfrac{\log b}{\log (b/a)}\right) & \text{if } 1 < a^2 \leqq b, \\ e^C \dfrac{\phi(b)}{b \log a} \log 2 & \text{if } a^2 > b \end{cases}$$

where C denotes the Euler constant and $\phi(b)$ is the Euler totient function.

Theorem 2. *There exists a set of natural numbers of positive (natural) density, consisting only of those numbers* n *with* G. C. D. $(n, ab) = 1$ *for which we have* $f(n; a, b) = 0$.

Proof of Theorem 2 can be carried out along the same lines of argument as given in Erdös [1]. In fact, we can find in general primitive prime factors[2] p_m of $a^m - b^m$ for $m = 2$, 3, 4, 8, 12, and 24. This is certainly possible unless $m = 2$ and $a + b = 2^e$ for some $e \geqq 1$, in which case $a - b$ is a non-zero even integer and we take, as we may, any prime factor p_2 of $a - b$. In any case the six primes p_m thus chosen are mutually distinct. none of them dividing the integer ab.

Now, every integer k satisfies at least one of the following congruences:

$k \equiv 0 \pmod 2$, $k \equiv 0 \pmod 3$, $k \equiv 1 \pmod 4$, $k \equiv 3 \pmod 8$, $k \equiv 7 \pmod{12}$, and $k \equiv 23 \pmod{24}$. For $m = 4$, 8, 12 and 24 we take integers a_m satisfying

1) Cf. K. A Rodosskiĭ: On the distribution of prime numbers in short arithmetic progressions. Izvestija Akad. Nauk SSSR Ser. Mat. **12** (1948), 123—128 (in Russian). As a matter of fact, we feel it inadequate to make use of this theorem of Rodosskiĭ for our present purpose.

2) A prime number p is a primitive prime factor of $a^m - b^m$, if p divides $a^m - b^m$ but does not divide $a^k - b^k$ for all k with $1 \leqq k < m$. For the condition on the existence of primitive prime factors one may refer e. g. to [5].

$$aa_m \equiv 1 \pmod{p_m}.$$

Then, for any natural number n which is congruent to 1 (mod p_2), to 1 (mod p_3), to a_4b (mod p_4), to $(a_8b)^3$ (mod p_8), to $(a_{12}b)^7$ (mod p_{12}), and to $(a_{24}b)^{23}$ (mod p_{24}), we see that for any k, $a^kn - b^k$ is divisible by one of the primes p^m ($m = 2, 3, 4, 8, 12, 24$). Since none of the primes p_m divide ab, and since the set of natural numbers n for which we have

$$a^kn - b^k = p_m$$

for some integers $k \geqq 1$ and m from among 2, 3, 4, 8, 12, 24, has density zero. This concludes the proof of Theorem 2.

REFERENCES

[1] P. ERDÖS: On integers of the form 2^k+p and some related problems. Summa Brasil. Math. **2** (1950), 113—123.

[2] P. ERDÖS: Quelques problèmes de la théorie des nombres. Monographies de l'Enseignement Mathématique No. 6, Genève (non-dated). Especially, Problem 54, pp. 121—122.

[3] P. ERDÖS: Résultats et problèmes en théorie des nombres. Séminaire Delange-Pisot-Poitou (14e année: 1972/73), Fasc. 2, Exp. No. 24, 7 pp. Secrétariat Mathématique, Paris (1973). MR **53** (1977), #243.

[4] W. E. MIENTKA and R. C. WEITZENKAMP: On f-plentiful numbers. J. Combinatorial Theory **7** (1969), 374—377.

[5] A. SCHINZEL: On primitive prime factors of a^n-b^n. Proc. Cambridge Phil. Soc. **58** (1962), 555—562.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received May 9, 1977)