STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1955-012

On almost primes

H.J.A. Duparc

1955

On almost primes

by

H.J.A. Duparc

Several authors [1] [2] proved the existence of an infinite number of composite m for which $2^{m-1} \equiv 1 \pmod{m}$. These numbers m are sometime called almost primes.

In this note it will be proved that if a is an arbitrary given integer > 1 there exist infinitely many composite m with

$$(1) \qquad a^{m-1} \equiv 1 \pmod{m}.$$

Such numbers m will be called almost primes. In the case a=2 a table of all such almost primes $< 10^8$ has been given by Poulet [3] .

Three proofs of this assertion will be given. The first runs similar to that of Sierpinski who proved that $M=2^m-1$ is almost prime if m is so; the second is a generalization of Jarden's method who used numbers of the form $2^{2^n} + 1$. Moreover a third proof is given which is shorter than either of the two others.

Theorem 1. For every integer $a>1$ there exists an almost prime m. Moreover to m the supplementary condition $(a-1,m)=1$ may be imposed.

Proof. For a=2 the number m=341 satisfies.

Let further a be an odd prime. Then one may take $m=\frac{a^{2a}-1}{a^2-1}$. In fact obviously m is composite. Further

$$\frac{a^{2a-2}-1}{a^2-1} = a^{2a-4} + \ldots + a^2+1 \equiv 1+\ldots+ 1 + 1 = a-1 \equiv 0 \pmod{2},$$

hence

$$2(a^2-1) \mid a^{2a-2}-1, \quad 2a \mid \frac{a^{2a}-a^2}{a^2-1} = m-1, \quad a^{2a}-1 \mid a^{m-1}-1$$

and consequently

$$m \mid a^{m-1}-1.$$

Moreover any prime divisor p of a-1 satisfies

$$m= \frac{a^{2a}-1}{a^2-1} = a^{2a-2}+\ldots+ a^2 + 1 \equiv 1 +\ldots+ 1 + 1 = a \equiv 1 \pmod{p},$$

hence $p \nmid m$ and $(a-1,m)=1$.

Finally consider the case a is composite. Then obviously $m=\frac{a^a-1}{a-1}$ is also composite and further

$$a \mid \frac{a^a-a}{a-1} = m-1, \text{ hence } m \mid a^a-1 \mid a^{m-1}-1$$

Moreover as before any prime divisor p of a-1 satisfies

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

$$m = \frac{a^a - 1}{a-1} = a^{a-1} + \ldots + a + 1 \equiv 1 + \ldots + 1 + 1 = a \equiv 1 \pmod{p},$$

hence $p \nmid m$ and $(a-1, m) = 1$.

Theorem 2. For every integer $a > 1$ there exist infinitely many a-almost primes.

Proof. Let m be a composite number satisfying (1) and $(a-1,m)=1$. Then

$$M = M(m) = \frac{a^m - 1}{a-1}$$

is also composite, satisfies also (1) and $(a-1,M)=1$.

The first assertion is obvious.

Further one has

$$m \mid a^{m-1} - 1 \mid a^m - a = (a-1)(M-1),$$

hence $m \mid M-1$ in virtue of $(a-1,m)=1$. Then $M \mid a^m - 1 \mid a^{M-1} - 1$.

The last assertion follows from the fact that every prime factor p of $a-1$ satisfies $p \nmid m$, hence

$$M = a^{m-1} + \ldots + a + 1 \equiv 1 + \ldots + 1 + 1 = m \not\equiv 0 \pmod{p}.$$

Now for a given $a > 1$ first introduce the number $m_0 = m$ of the preceding theorem. Then by the above argument every member of the sequence $m_0, m_1, \ldots$ defined by

$$m_{h+1} = M(m_h) \qquad (h = 0, 1, \ldots)$$

is an almost prime.

Remark. If m_h possesses s different prime factors, then m_{h+1} will have at least $s+1$. Consequently there exist infinitely many almost primes with at least s different prime factors.

Now the second proof of the existence of infinitely many almost primes will be given.

Theorem 3. Consider the sequence of integers $u_h = (a^{a^h} - 1)/(a^{a^{h-1}} - 1)$ $(h = 1, 2, \ldots)$. Then for positive integers n and m satisfying $n < m \leqq a^{n-1}$ one has $u_n u_m \mid a^{u_n u_m - 1} - 1$.

Proof. If $h \leqq a^{k-1}$ one has $a^h \mid a^{a^k} - a^{a^{k-1}} \mid u_k - 1$. Hence $u_h \mid a^{a^h} - 1 \mid a^{u_k - 1} -$

Consequently

$$u_n \mid a^{u_n - 1} - 1, \quad u_m \mid a^{u_n - 1} - 1, \quad u_n \mid a^{u_m - 1} - 1, \quad u_m \mid a^{u_m - 1} - 1,$$

which leads to

$$(2) \quad u_n \mid a^{u_n u_m - 1} - 1, \quad u_m \mid a^{u_n u_m - 1} - 1.$$

Further $(u_n, u_m) = 1$. In fact let p be an arbitrary prime factor of u_n.

Then $p \mid a^{a^{m-1}}-1$ since $m-1 \geqq n$. Now

$$u_m = a^{a^{m-1}(a-1)}+\dots+a^{a^{m-1}}+1 \equiv 1+\dots+1+1=a \not\equiv 0 \pmod p.$$

Thus $p \nmid u_m$ and $(u_n,u_m)=1$.

Then (2) yields $u_n u_m \mid a^{u_n u_m -1}-1$ and infinitely many almost primes $u_n u_m$ are found.

Remark. For $n_1 < n_2 \dots < n_s < a^{n_1-1}-1$ one finds in a similar way from (2) that the number $u_{n_1} u_{n_2} \dots u_{n_s}$ is an almost prime. Hence there exist infinitely many almost primes with at least s different prime factors.

Finally a third proof will be given, first in its most simple version, then in a little more complicated generalized form.

Theorem 4. Let p be a prime not dividing a^2-1. Then $m=\dfrac{a^{2p}-1}{a^2-1}$ is an almost prime.

Proof. First it is proved that m-1 is even. In fact if a is even, obviously m is odd and then m-1 even. If however a is odd one has

$$m = a^{2p-2}+\dots+a^2+1 \equiv 1+\dots+1+1=p \equiv 1 \pmod 2.$$

Further $p \mid a^p-a \mid a^{2p}-a^2$, hence $p \mid \dfrac{a^{2p}-a^2}{a^2-1} = m-1$ in virtue of $p \nmid a^2-1$. Consequently $2p \mid m-1$. Then

$$m \mid a^{2p}-1 \mid a^{m-1}-1.$$

Finally $m=\dfrac{a^p-1}{a-1} \cdot \dfrac{a^p+1}{a+1}$ is composite, which proves the theorem.

Remark. In the case p=2 the number m is also almost prime provided a^2+1 be composite.

In fact since $2 \nmid a^2-1$ the number a is even, hence $4 \mid a^2=m-1$

$$m = a^2+1 \mid a^4-1 \mid a^{m-1}-1$$

This theorem gives again the existence of infinitely many almost primes. Here they are of the form $m=\dfrac{a^{2p}-1}{a^2-1}$ where p runs through the infinite set of all primes.

The above mentioned generalization of theorem 4 is the following:

If an integer k satisfies the relation $(k,a^k-1)=1$, then for every prime number p with $p \nmid k(a^k-1)$, $k \mid a^{kp}-a^k$ the number $m=\dfrac{a^{kp}-1}{a^k-1}$ is almost prime. (The special case k=2 is the above treated more simple theorem).

In fact one has $k \mid \dfrac{a^{kp}-a^k}{a^k-1} = m-1$ and further using Fermat's theorem $p \mid a^{kp}-a^k$, hence $p \mid m-1$ since $p \nmid a^k-1$. Consequently $kp \mid m-1$ and $m \mid a^{kp}-1 \mid a^{m-1}-1$. Moreover obviously m is composite.

Applications. The case k=3 requires that $3 \nmid a^3-1$, i.e. $a \not\equiv 1 \pmod 3$.

Then if $p\neq 2$, $p\neq 3$, $p\nmid a^3-1$ one has $a^{3p}-a^3\equiv a-a=0 \pmod 3$, and all conditions of the theorem being satisfied one concludes that $m=\frac{a^{3p}-1}{a^3-1}$ is an almost prime.

The case k=4 requires a^4-1 to be odd, hence a even. Then for every odd prime p with $p\nmid a^4-1$ one has $a^{4p}\equiv a^4 \pmod 4$ and the theorem gives that $m=\frac{a^{4p}-1}{a^4-1}$ is almost prime.

The case k=5 requires $5\nmid a^5-1$, i.e. $a\not\equiv 1 \pmod 5$. Further $p\neq 5$, $p\nmid a^5-1$. Moreover $5\mid a^{5p}-a^5$ will hold for all a if $p\equiv 1 \pmod 4$, whereas in the case $p\equiv 3 \pmod 4$ one has to take $a\equiv 0$, 2 or 3 (mod 5). Under these conditions $m=\frac{a^{5p}-1}{a^5-1}$ is almost prime.

As a last example consider the case k=6. Then $2\nmid a^6-1$, $3\nmid a^6-1$ gives $6\mid a$. Further one has to take $p\neq 2$, $p\neq 3$, $p\nmid a^6-1$. Since then $6\mid a^{6p}-a^6$ the number $m=\frac{a^{6p}-1}{a^6-1}$ is almost prime.

---

[1] W. Sierpiński, Remarque sur une hypothèse des chinois concernant les nombres $\frac{2^n-2}{n}$, Coll. Math. I (1947), 9.

[2] D. Jarden, Existence of an infinitude of composite n for which $2^{n-1}\equiv 1 \pmod n$, Riv. Lemat. 4(1950), 65-67.

[3] P. Poulet, Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à 100 000 000, Sphinx 8(1938), 42-52. Confer also

[4] H.J.A. Duparc, On Mersenne numbers and Poulet numbers, Rapport ZW 1953-001, Mathematisch Centrum.

[5] H.J.A. Duparc, On Carmichael numbers, Poulet numbers, Mersenne numbers and Fermat numbers, Rapport ZW 1953-004, Mathematisch Centrum.
An estimation of the number of almost primes in the sense of Poulet has been given by

[6] P. Erdös, On almost primes, Amer. Math. Monthly 57 (1950), 404-407.