A014117 and related OEIS sequences

Don Reble

2018 April

Contents

1 Introduction

From the OEIS[1]

```
%I A014117
%S 1,2,6,42,1806
%N Numbers n such that m^(n+1) == m (mod n)
   holds for all m.
%O 1,2
%A David Broadhurst
```

Robert Israel and Thomas Ordowski note that A014117 is the

P1: squarefree terms of A124240

Max Alekseyev notes other properties of the sequence values:

P2: for $n > 1$, n is an even squarefree number
P3: The set P of all prime divisors of such n has this property: if p is in P, then $p-1$ is a product of distinct elements of P. This set is $P = \{2, 3, 7, 43\}$, implying that the sequence is finite and complete.
P4: n such that $\sum_{i=1}^{n} i^n \equiv 1 \bmod n$
P5: $\sum n/p \equiv -1 \bmod n$, summing over primes p such that $p \leq n$ and $(p-1) \mid n$
P6: n such that n divides the denominator of the n-th Bernoulli number B_n (see A106741)

A further property from Derek Orr, noted in the equal sequence A242927:

P7: n such that $\displaystyle\sum_{i=k}^{k+n-1} i^n$ is prime for some k

2 Review and Preliminaries

Fermat's little theorem

If p is prime, $a^p \equiv a \bmod p$; and $a^{p-1} \equiv 1$, unless $a \equiv 0$.

(This is almost the defining property of A014117, as Broadhurst notes.)

Sums of $i^n \bmod p$

Theorem 119 of [2] shows that for prime p,

$$\sum_{i=1}^{p-1} i^n \bmod p \equiv \begin{cases} (p-1) \mid n \rightarrow & p-1 \\ (p-1) \nmid n \rightarrow & 0 \end{cases}$$

That sum could include the $i = 0$ term, using all i-values modulo p. Indeed, the index can run through any p consecutive values. For any non-negative k,

$$\sum_{i=0 \text{ or } 1}^{p-1} i^n \bmod p \equiv \sum_{i=k}^{k+p-1} i^n$$

Prime reciprocal sums

Let p_i be the elements of a set of primes, let a be an integer, and let $b = \sum_i a/p_i$.
b is a rational number, and might be an integer.

The value $b\prod_i p_i = a\sum_i \frac{\prod_i p_i}{p_i}$
is an integer. For each i, the summed terms include $i-1$ multiples of p_i, and one non-multiple: the sum is not a multiple of any p_i.

So b is an integer just if each $p_i \mid a$: $\prod p_i \mid a$.

3 P1 proof

Let X be the set of integers x such that

- if prime $p \mid x$, then $(p-1) \mid x$;
- x is squarefree.

OEIS A124240 (mentioned in property P1) is defined by just the first property.

An *X-prime* is a prime that divides an element of set X.

Obviously $2 \in X$ and 2 is an X-prime.

Given a set P of X-primes, one can combine subsets to seek more. If $1+\prod P$ is prime, it is an X-prime.

P	$1+\prod P$	P	$1+\prod P$
2	**3**	2,43	$87 = 3\cdot 29$
2,3	**7**	2,3,43	$259 = 7\cdot 37$
2,7	$15 = 3\cdot 5$	2,7,43	$603 = 3\cdot 3\cdot 67$
2,3,7	**43**	2,3,7,43	$1807 = 13\cdot 139$

The process finds 3, then 7, then 43; each other try finds a composite dead-end.

Consider the set Y of X-primes minus $\{2,3,7,43\}$. If non-empty, Y has a least member y; y divides an element $x \in X$; $(y-1) \mid x$; and $y-1$ is a squarefree product of X-primes.
The prime divisors of $y-1$ are smaller than y, so not in Y: they are in $\{2,3,7,43\}$. But those possibilities are exhausted. There is no such y, and Y is empty.

The X-primes are $\{2,3,7,43\}$.

Furthermore,
$43 \mid x$ implies that $42 \mid x$ (2,3,7 are divisors);
$7 \mid x$ implies that $6 \mid x$ (2,3 are divisors);
$3 \mid x$ implies that $2 \mid x$.

$X = \{1,2,6,42,1806\}$.

Property P1: defines the listed elements of A014117.

4 P2 & P3 proofs

Definition: n such that for all m, $m^{n+1} \equiv m \bmod n$

Suppose that for some prime p, $p^2 \mid n$. Then $m^{n+1} \equiv m \bmod p^2$.
This is true all for m, particularly when $m = p$: $p^{n+1} \equiv p \bmod p^2$. No, $n+1 \geq 2$, so it's $0 \bmod p$, and the supposition is false.

Theorem 2: n is squarefree.

Let p be a prime factor of n. Then $m^{n+1} \equiv m \bmod p$. This is true for all m, particularly when m is a primitive root of p, whence $m^a \equiv m$ only when $a \equiv 1 \bmod (p-1)$.
Therefore $n+1 \equiv 1 \bmod (p-1)$, and $n \equiv 0$.

Theorem 3: if prime $p \mid n$, then $(p-1) \mid n$.

If $n > 1$, n is divisible by a prime.
If odd prime $q \mid n$, then $q-1 \mid n$ and $2 \mid q-1$.
If even prime $2 \mid n$, then $2 \mid n$.
n is even.

Property P2: For $n > 1$, n is an even squarefree number.

Theorems 2 and 3 together imply that A014117 is a subset of X. Calculations show that each value works.

Theorem 0: A014117 = 1,2,6,42,1806.

Property P3 is proven.

Property P1: can be a definition of A014117.

5 P4 & P7 proofs

Let $S(n) = \sum_{i=1}^{n} i^n$.

Let n be an integer such that $S(n) \equiv 1 \bmod n$.

Let p be a prime dividing n: $n = mp$.
$S(mp) \bmod p = \sum_{i=1}^{mp} i^{mp} \bmod p \equiv m \cdot \sum_{i=0}^{p-1} i^{mp}$, since each i can be replaced by $i \bmod p$, and each reduced i-value occurs m times. From section 2, this is congruent to $m\cdot(p-1)$ if $(p-1) \mid n$; or else 0.

So if $p \mid n$, then $n \equiv 0 \bmod (p-1)$.

Theorem 4a: if prime $p \mid n$ then $(p-1) \mid n$.

Suppose that for some prime p, $p^2 \mid n$: $n = mp^2$. As before, $S(mp^2) \bmod p \equiv mp \cdot \sum_{i=0}^{p-1} i^n$, which is divisible by p.

Theorem 4b: n is squarefree.

Theorems 4a and 4b together imply that $S \subseteq X$. Calculations show that each value works.

Property P4: can be a definition of A014117.

Let $T(n,k) = \sum_{i=k}^{k+n-1} i^n$

We have these data from Orr:

n	k	$T(n,k)$
1	2	2
2	1	5
6	4	977611
42	99	5 18750 71360 65560 08930 68812 01989 63767 29562 90824 50510 36490 50056 91739 06968 89594 20495 98772 64141

The first three T values are obviously prime. For the fourth, appendix A has a "P-1" proof.

Henceforth, let $n \geq 3$.

$T(n,k) \geq T(n,0) > (n-1)^n > n$.

Let p be a prime dividing n: $n = mp$. As before, $T(mp,k) \bmod p = \sum_{i=k}^{k+mp-1} i^{mp} \bmod p \equiv$ $m \cdot \sum_{i=0}^{p-1} i^{mp}$, congruent to 0 if $(p-1) \not| \, n$.

If $T(mp,k)$ is prime, it is too large to be the prime p: mp must be divisible by $(p-1)$.

Theorem 7a: For $n \geq 3$: if $p \mid n$ and $T(n,k)$ is prime, then $(p-1) \mid n$.

Suppose that for some prime p, $p^2 \mid n$: $n = mp^2$. As before, $T(mp^2,k) \bmod p$ is a multiple of mp and of p, and is greater than p.

Theorem 7b: For $n \geq 3$: if $p^2 \mid n$ then $T(n,k)$ is composite.

Theorem 7c: The set of n's for which $T(n,k)$ is prime is a subset of X.

$T(1806, 3081)$ is a strong probable-prime. At least, there are no strong-witnesses in the first 100 primes.

Property P7: is probably true, and could be a definition of A014117.

6 P5 proof

The P5 summation, $\sum n/p \equiv -1 \bmod n$, uses each prime p such that $p \leq n$ and $(p-1) \mid n$. The sum is an integer just if each $p \mid n$.

Let $n > 1$, and let p be a prime dividing n. To make the sum a non-multiple of p, we need a term that divides-out that prime: so $(p-1) \mid n$, and $p^2 \not| \, n$.

Therefore n is squarefree, and for each $p \mid n$, $(p-1) \mid n$. The set of such n's is a subset of X, Calculations show that each value works. (For $n = 1$, the sum has no terms: take it to be $0 = n - 1$.)

Property P5: can be a definition of A014117.

Furthermore, in each case $\sum n/p = n - 1$. That also can define A014117; the same proof applies.

7 P6 proof

Von Staudt's theorem, number 118 of [2], states

$$(-1)^k B_{2k} \equiv \sum 1/p \bmod 1$$

summing over primes p such that $p-1 \mid 2k$. That determines the B_{2k} denominator.

Such denominators are therefore squarefree (as Hardy&Wright note).

> H&W write β_k instead of B_k, and B_k instead of B_{2k}.

Let D_n be the denominator of B_n.

Of course $n = 1$ divides D_1. For larger odd n, $B_n = 0/1$, and $n \not| \, 1$.

Let n be an even number that divides D_n, and let p be a prime dividing n: $p \mid D_n$. Therefore p is included in that summation, so $(p-1) | n$.

Theorem 6: Such an n is squarefree; and if prime $p \mid n$, then $(p-1) \mid n$.

Therefore $n \in X$; calculations show that each value works.

Property P6: can be a definition of A014117.

A $T(42, 99)$ is prime

Here's a "P-1" proof for $a = T(42, 99)$. Each base (for $x^{(p-1)/f}$) is 2, unless shown.

p	p-1 factor,base
a	2 − 3 − 5 − 7 − 13 − 53 − h − b
b	2 − 3 − 79 − i − c
c	2,5 − 521 − 1663 − 87557 − d
d	2,3 − 17 − 1583 − f − e
e	2 − 7 − 11,5 − 56041 − g
f	2,3 − 3,11 − 59 − 1252357 − 67373239
g	2 − 3,3 − 3940499 − 96670153
h	2 − 7 − 159673 − 1931953451
i	2,5 − 2909 − 4345087

```
a= 5 18750 71360 65560 08930 68812 01989
     63767 29562 90824 50510 36490 50056
     91739 06968 89594 20495 98772 64141
b=                               13836 07033
     87001 00317 19250 01625 21525 38706
     93348 24570 88594 01525 80203 88187
c=      11 54681 54858 90651 83829 55328
     50710 66466 88709 75798 69163 87767
d=                   76104 68365 53864
     22033 86052 23524 42716 34821 42553
e=         1183 51216 27356 19172 16803
f=                   29 86887 30059 10343
g=                   13 71343 10841 48493
h=                    4 31873 12473 41323
i=                          2 52797 16167
```

Smaller primes are verified by trial-division.

References

[1] Neil Sloane, *The Online Encyclopedia of Integer Sequences*, `http://oeis.org`

[2] G H Hardy, E M Wright, *An Introduction to the Theory of Numbers* 5th edition, Oxford University Press, 1983.