Comments on OEIS A081215

by Mathew Englander, October 19, 2020.

$a(n) = (n^{n+1} + (-1)^n)/(n+1)^2$

a(n) = A081209(n) / (n+1)

see also A110567 (see comments therein), A076951 (ditto), A273319, A193746, A060073.

Theorems (proved below in this document):

I. For n > 0, a(n) ≡ (−1)^n (mod n). Hence a(n)+1 or a(n)−1 is a multiple of n, for n odd and even respectively.

II. For even n, a(n) ≡ 1 (mod n+1).
For odd n, a(n) ≡ floor(n/2) = (n−1)/2 (mod n+1).
Corollaries: for odd m, m divides a(m−1)−1; for even m>0, ½m divides a(m−1)+1; for all m>0, m divides a(2m−1)+1.

III. For n > 2, a(n) mod (n−1) = floor(n/2).
Corollaries: for m even, a(m+1) is a multiple of ½m; for all m, a(2m+1) and a(2m)−1 are multiples of m.

IV. 4m divides a(2m)−1 for all m.

V. In base n, a(n) has n-1 digits, which are (beginning from the left): n-2, 2, n-4, 4, n-6, 6, and so on, except that if n is even the rightmost digit is 1 instead of 0. In that case, the other digits form a palindrome with every even digit from 2 to n-2 appearing twice. For example, a(14) in base 14 is c2a486684a2c1. If n is odd, then all digits from 1 to n-1 occur exactly once (with n-1 as the rightmost digit). For example, a(15) in base 15 is d2b496785a3c1e.

VI. a(n) mod 12 =
0, if n mod 24 = 1
1, if n mod 24 = 0, 2, 6, 8, 12, 14, 18, or 20
2, if n mod 24 = 5 or 21
3, if n mod 24 = 7
5, if n mod 24 = 3, 4, 10, 11, 16, or 22

6, if n mod 24 = 13
8, if n mod 24 = 9 or 17
9, if n mod 24 = 19
11, if n mod 24 = 15 or 23

Corollaries:
No term of the sequence is congruent to 4, 7, or 10 (mod 12);
a(n+3) - a(n+10) == floor(n/2) (mod 6) for n >= -3;
a(n) - a(n+2) == n (mod 6) for n >= 0;
a(n-4) - a(n) == 2n (mod 12) for n >= 4.

VII. If p is an odd prime, h is a nonnegative integer, k is a positive integer, and j is an integer greater than or equal to –hp, then
$a(hp^k + j) \equiv a(hp + j) \pmod{p}$.

VIII. For any odd prime p, and any positive integer k, at least one of the following is true: p divides k, p divides k+1, p divides a(kp–k–1).

IX. For any odd prime p, p divides a(p-2), a(2p+1), a(2p-2)+1. Indeed, p divides a(p^k-2), a(2kp+1), and a(2p^k-2)+1 for any positive integer k.

X. For any prime p, and any positive integers k and h such that h*p > 2, $a(hp^k - 2) \equiv (1 - 2^{h-1})*(-1)^h \pmod{p}$. For example: $a(5p^k - 2) \equiv 15 \pmod{p}$; $a(10p^k - 2) \equiv -511 \pmod{p}$.

XI. For any prime p > 3 and any positive integer k,
if $p \equiv 1 \pmod{3}$ then $a(p^k - 3) \equiv (1-p)/6 \pmod{p}$; and
if $p \equiv -1 \pmod{3}$ then $a(p^k - 3) \equiv (1+p)/6 \pmod{p}$.
For any odd prime p, any positive integer k, and any odd integer h > 1, $a(hp^k - 3) \equiv (p+z)/2 \pmod{p}$, where $z = (9 - 3^h)/18$. For example, $a(5p^k - 3) \equiv (p - 13)/2 \pmod{p}$.
For any odd prime p, any positive integer k, and any positive even number h such that h*p > 6,
$a(hp^k - 3) \equiv (3^h - 9)/36 \pmod{p}$.
For example, $a(10p^k - 3) \equiv 1640 \pmod{p}$.

XII. Suppose k and m are positive integers. Then,
For even k:
$a(km) \equiv 1 \pmod{m}$
$a(km+1) \equiv 0 \pmod{m}$
$a(km-1) \equiv -1 \pmod{m}$

For odd k:
$a(km) \equiv (-1)^m \pmod{m}$
$a(km+1) \equiv \text{ceiling}(m/2) \pmod{m}$
$a(km-1) \equiv 1 \pmod{m}$ for m odd
$a(km-1) \equiv m/2 - 1 \pmod{m}$ for m even

XIII. For $n > 2$, $a(n) \bmod (n^2 + 1) = r(n)$, where
$r(n)$ is defined as follows for h = 0, 1, 2, ...:
$r(4h) = 8h^2 - 2h + 1$
$r(4h+1) = 8h^2 + 8h + 2$
$r(4h+2) = 8h^2 + 6h + 1$
$r(4h+3) = 8h^2 + 12h + 5$
Another way of defining $r(n)$ is this: for $n>3$,
$r(n) = r(n-1) - r(n-2) + r(n-3) - (n \bmod 4) + (4n - 5)(n \bmod 2) + 1$
We could also define $r(n)$ like this:
For $n \bmod 4 = 0$, $r(n) = \frac{1}{2}(n^2 - n + 2)$
For $n \bmod 4 = 1$, $r(n) = \frac{1}{2}(n^2 + 2n + 1)$
For $n \bmod 4 = 2$, $r(n) = \frac{1}{2}(n^2 - n)$
For $n \bmod 4 = 3$, $r(n) = \frac{1}{2}(n^2 + 1)$

Conjectures:

XIV. [Conjecture]:
For $n > 2$, $a(n) \bmod (n^3 - 1) = r(n)$, where
$r(n)$ is defined as follows for h = 0, 1, 2, ...:
$r(6h) = 108h^3 + 18h^2 - 3h$
$r(6h+1) = 108h^3 + 18h^2 + 3h$
$r(6h+2) = 108h^3 + 162h^2 + 69h + 8$
$r(6h+3) = 108h^3 + 126h^2 + 45h + 5$
$r(6h+4) = 108h^3 + 234h^2 + 171h + 41$
$r(6h+5) = 108h^3 + 270h^2 + 225h + 62$

We can also write r(n) as follows:

For n mod 6 = 0, $r(n) = \frac{1}{2}(n^3 + n^2 - n)$
For n mod 6 = 1, $r(n) = \frac{1}{2}(n^3 - 2n^2 + 2n - 1)$
For n mod 6 = 2, $r(n) = \frac{1}{2}(n^3 + 3n^2 - n - 2)$
For n mod 6 = 3, $r(n) = \frac{1}{2}(n^3 - 2n^2 + 1)$
For n mod 6 = 4, $r(n) = \frac{1}{2}(n^3 + n^2 + n - 2)$
For n mod 6 = 5, $r(n) = \frac{1}{2}(n^3 - 1)$

XV. [Conjecture]:

For n > 4, a(n) mod (n^4 + 1) = r(n), where
r(n) is defined as follows for h = 0, 1, 2, ...:

```
r(8h)   = 2048*h^4 -  256*h^3 +  32*h^2  -  4*h + 1
r(8h+1) = 2048*h^4 + 1536*h^3 + 320*h^2  + 32*h + 2
r(8h+2) = 2048*h^4 + 1280*h^3 + 288*h^2  + 28*h + 1
r(8h+3) = 2048*h^4 + 4096*h^3 + 2816*h^2 + 816*h + 87
r(8h+4) = 2048*h^4 + 3328*h^3 + 1952*h^2 + 484*h + 41
r(8h+5) = 2048*h^4 + 5632*h^3 + 5760*h^2 + 2592*h + 434
r(8h+6) = 2048*h^4 + 5888*h^3 + 6304*h^2 + 2980*h + 525
r(8h+7) = 2048*h^4 + 7168*h^3 + 9408*h^2 + 5488*h + 1201
```

Another way of defining r(n) is:

if n mod 8 is 0, $r(n) = \frac{1}{2}(n^4 - n^3 + n^2 - n + 2)$
if n mod 8 is 1, $r(n) = \frac{1}{2}(n^4 + 2n^3 - 2n^2 + 2n + 1)$
if n mod 8 is 2, $r(n) = \frac{1}{2}(n^4 - 3n^3 + 3n^2 - n)$
if n mod 8 is 3, $r(n) = \frac{1}{2}(n^4 + 4n^3 - 2n^2 + 3)$
if n mod 8 is 4, $r(n) = \frac{1}{2}(n^4 - 3n^3 + n^2 + n - 2)$
if n mod 8 is 5, $r(n) = \frac{1}{2}(n^4 + 2n^3 - 2n + 3)$
if n mod 8 is 6, $r(n) = \frac{1}{2}(n^4 - n^3 - n^2 + n)$
if n mod 8 is 7, $r(n) = \frac{1}{2}(n^4 + 1)$

Verified for n up to 51000, i.e. h up to 6375.

XVI. [Conjecture]:

For n > 5, a(n) mod (n^5 - 1) = r(n), where
r(n) is defined as follows for h = 0, 1, 2, ...:

```
r(10h)   = 50000*h^5 +   5000*h^4 -    500*h^3 +     50*h^2 -      5*h
r(10h+1) = 50000*h^5 +  15000*h^4 +   2000*h^3 +    100*h^2 +      5*h
r(10h+2) = 50000*h^5 +  65000*h^4 +  30500*h^3 +   6850*h^2 +    755*h +    32
r(10h+3) = 50000*h^5 +  55000*h^4 +  23000*h^3 +   4400*h^2 +    345*h +     5
r(10h+4) = 50000*h^5 + 125000*h^4 + 118500*h^3 +  54250*h^2 +  12125*h +  1064
r(10h+5) = 50000*h^5 + 105000*h^4 +  86000*h^3 +  34000*h^2 +   6365*h +   434
r(10h+6) = 50000*h^5 + 165000*h^4 + 215500*h^3 + 139450*h^2 +  44775*h +  5713
r(10h+7) = 50000*h^5 + 165000*h^4 + 217000*h^3 + 142200*h^2 +  46435*h +  6045
r(10h+8) = 50000*h^5 + 205000*h^4 + 336500*h^3 + 276350*h^2 + 113525*h + 18659
r(10h+9) = 50000*h^5 + 225000*h^4 + 405000*h^3 + 364500*h^2 + 164025*h + 29524
```

Another way of defining r(n) is:

if n mod 10 is 0, $r(n) = \frac{1}{2}(n^5 + n^4 - n^3 + n^2 - n)$

if n mod 10 is 1, $r(n) = \frac{1}{2}(n^5 - 2n^4 + 2n^3 - 2n^2 + 2n - 1)$

if n mod 10 is 2, $r(n) = \frac{1}{2}(n^5 + 3n^4 - 3n^3 + 3n^2 - n - 2)$

if n mod 10 is 3, $r(n) = \frac{1}{2}(n^5 - 4n^4 + 4n^3 - 2n^2 + 1)$

if n mod 10 is 4, $r(n) = \frac{1}{2}(n^5 + 5n^4 - 3n^3 + n^2 + n - 4)$

if n mod 10 is 5, $r(n) = \frac{1}{2}(n^5 - 4n^4 + 2n^3 - 2n + 3)$

if n mod 10 is 6, $r(n) = \frac{1}{2}(n^5 + 3n^4 - n^3 - n^2 + 3n - 4)$

if n mod 10 is 7, $r(n) = \frac{1}{2}(n^5 - 2n^4 + 2n^2 - 2n + 1)$

if n mod 10 is 8, $r(n) = \frac{1}{2}(n^5 + n^4 + n^3 - n^2 + n - 2)$

if n mod 10 is 9, $r(n) = \frac{1}{2}(n^5 - 1)$

XVII. Conjecture: Suppose k is any positive integer, and n an integer with n > k. Then a(n) mod $(n^k + (-1)^k)$ can be expressed by a set of 2k polynomials in n of degree k, a different polynomial depending on n mod 2k.

XVIII. [Conjecture]:

For n odd, n>2, a(n) mod $(n-1)^2/2 = (n-1)/2$

i.e. for m > 0, a(2m+1) mod $2m^2 = m$

XIX. [Conjecture]:

For any nonnegative integer n,

$2*a(n) \equiv n^n - n*(-1)^n \pmod{n^2 + 1}$.

XX. [Conjecture]:

For any integer $n \geq 2$,

a(2m+1) mod $m^3 = m$.

XXI. [Conjecture]:

For a prime p other than 2 or 3,

$a((p-3)/2) \equiv 0, 8, \text{ or } -8 \pmod{p}$.

XXII. [Compilation of miscellaneous conjectures.]

FORMULAS

There are a few different ways to express a(n) as a summation involving binomial coefficients. They may be useful in different contexts.

Let m = n+1. Now

$$n^{(n+1)} = (m-1)^m = \sum_{k=0}^{m} (-1)^{(m-k)} * \binom{m}{k} * m^k = (-1)^m + \sum_{k=1}^{m} (-1)^{(m-k)} * \binom{m}{k} * m^k \quad ,$$

and since (–1)^n = –(–1)^m,

$$n^{(n+1)} + (-1)^n = \sum_{k=1}^{m} (-1)^{(m-k)} * \binom{m}{k} * m^k$$

, and since binom(m,1)*m = m^2,

$$n^{(n+1)} + (-1)^n = (-1)^{(m-1)} * m^2 + \sum_{k=2}^{m} (-1)^{(m-k)} * \binom{m}{k} * m^k$$

, and dividing both sides by (n+1)^2 = m^2,

$$\frac{n^{(n+1)} + (-1)^n}{(n+1)^2} = (-1)^{(m-1)} + \sum_{k=2}^{m} (-1)^{(m-k)} * \binom{m}{k} * m^{(k-2)} \quad ,$$

but we can also note that the final two terms in the summation here (i.e., for k = m–1 and k = m), we have:

$(-1)^1 * \binom{m}{m-1} * m^{(m-3)} + (-1)^0 * \binom{m}{m} * m^{(m-2)}$, which is 0 since $\binom{m}{m-1}$ = m and $\binom{m}{m}$ = 1. So when it’s convenient we can ignore the final two terms of the summation, and make the summation from k = 2 to k = m – 2:

$$a(n) = (-1)^{(m-1)} + \sum_{k=2}^{m-2} (-1)^{(m-k)} * \binom{m}{k} * m^{(k-2)}$$

, for m > 3. Substituting m = n+1 we get:

(i) $a(n) = (-1)^n + \sum_{k=2}^{n-1} (-1)^{(n+1-k)} * \binom{n+1}{k} * (n+1)^{(k-2)}$ for n > 2

(ii) $a(n) = (-1)^n + \sum_{k=2}^{n+1} (-1)^{(n+1-k)} * \binom{n+1}{k} * (n+1)^{(k-2)}$ for n > 0

(iii) $a(n) = (-1)^n + \sum_{k=0}^{n-3} (-1)^{(n+1-k)} * \binom{n+1}{k+2} * (n+1)^k$ for n > 2

(iv) $a(n) = (-1)^n + \sum_{k=0}^{n-1} (-1)^{(n+1-k)} * \binom{n+1}{k+2} * (n+1)^k$ for n > 0

relevant link:
https://math.stackexchange.com/questions/3052427/prove-that-nn-1-1-is-divisible-by-n-12

For other formulas, see proof of Theorem V, below.

I. For n > 0, a(n) ≡ (−1)^n (mod n). Hence a(n)+1 or a(n)−1 is a multiple of n, for n odd and even respectively.

PROOF: In the definition of a(n), we can multiply both sides by (n+1)^2 to get:

(n+1)^2 * a(n) = n^(n+1)+(−1)^n

Considered modulo n, this simplifies to:
a(n) ≡ (−1)^n (mod n) Q.E.D.

This is a special case of Theorem XXII, which says
a(km) ≡ (−1)^(km) (mod m)

It follows that if m is odd, m divides a(m)+1, and if m is even and positive, m divides a(m)−1. If m=0, a(m)−1 = 0; in that case it is awkward to say “m divides 0” since it implies we are dividing 0 by 0 (see https://math.stackexchange.com/q/666103).
To get around this just say:
a(n)+1 is a multiple of n if n is odd;
a(n)−1 is a multiple of n if n is even.

II. For even n, a(n) ≡ 1 (mod n+1).
For odd n, a(n) ≡ floor(n/2) = (n−1)/2 (mod n+1).
Corollaries: for odd m, m divides a(m−1)−1; for even m>0, ½m divides a(m−1)+1; for all m>0, m divides a(2m−1)+1.

Proof: First observe that the statement is true for n=0. Now suppose n is positive, and apply formula **(iv)** from above:

$$a(n)=(-1)^n+\sum_{k=0}^{n-1}(-1)^{n+1-k}*\binom{n+1}{k+2}*(n+1)^k \quad \text{for } n>0$$

Considering this mod n+1, we can disregard all terms of the summation with k ≥ 1, since they are all multiples of n+1. That leaves us with:

a(n) ≡ (−1)^n + (−1)^(n+1−0) * C(n+1,2) * (n+1)^0 (mod n+1)

If n is even then C(n+1, 2) = n(n+1)/2 is a multiple of n+1 and we get:
a(n) ≡ (−1)^n = 1 (mod n+1).

If n is odd, say n=2r−1, and
C(n+1, 2) = (2r−1)(2r)/2 = r(2r−1) ≡ −r (mod n+1),
because n+1=2r.

Now a(n) ≡ $(-1)^n$ + $(-1)^{n+1}$(−r) (mod n+1)
= −1 − r, since n is odd
= −1 − ½(n+1)
≡ (n + 1) − 1 − ½(n+1) (mod n+1)
= ½(n−1) = floor(n/2) (mod n+1) Q.E.D.

These are special cases of Theorem XII below, which says:
a(km−1) ≡ m/2 − 1   (mod m), for k odd and m even
a(km−1) ≡ 1   (mod m), for k odd and m odd

Setting m = n+1 yields:
m divides a(m−1)−1 for m odd, and
for m even: a(m−1) ≡ (m−2)/2 = ½m − 1 (mod m)
a(m−1)+1 ≡ ½m (mod m)
and therefore ½m divides a(m−1)+1 for m even, m > 0,
and if we say m = 2q, we get:
q divides a(2q−1)+1 for all q > 0.
In fact we can say a(2q−1)+1 is an odd multiple of q, for all positive integers q.

III. For n > 2, a(n) mod (n–1) = floor(n/2).

Corollaries: for m even, a(m+1) is a multiple of ½m; for all m, a(2m+1) and a(2m)–1 are multiples of m.

Proof: From the definition of a(n), we get
(n+1)^2 * a(n) = n^(n+1) + (–1)^n.

Now when we consider this mod n–1, we can replace the n+1 on the left side by 2, and the first n on the right side by 1:

4 * a(n) ≡ 1 + (–1)^n (mod n–1)

4 * a(n) ≡ 2 (mod n–1) if n is even
4 * a(n) ≡ 0 (mod n–1) if n is odd

We consider the two cases separately. First suppose n is even: so we have n even and 4a(n) ≡ 2 (mod n-1); we need to prove a(n) ≡ n/2 (mod n-1).

Well, n–1 is odd, so we can divide both sides of the congruence by 2, yielding 2a(n) ≡ 1 (mod n-1). Now since n is even, we can multiply both sides by n/2, giving us n*a(n) ≡ n/2 (mod n-1). But n ≡ 1 so now we have a(n) ≡ n/2 (mod n-1), which proves the theorem for n even.

But I can't get that method to work for n odd. The congruence 4a(n) ≡ 0 (mod n-1) allows up to four different solutions for a(n).

Instead, try a different way using the summation formulas for a(n).

Consider the binomial expansion of (x – 1)^m where x=2:

$$(2-1)^m=\sum_{k=0}^{m}(-1)^{(m-k)}\cdot\binom{m}{k}\cdot 2^k \quad .$$

The left-hand side is 1. Then (assuming m > 1) we can pull out the values for k=0 and k=1 to get this:

$$1=(-1)^m\cdot\binom{m}{0}\cdot 2^0+(-1)^{(m-1)}\cdot\binom{m}{1}\cdot 2^1+\sum_{k=2}^{m}(-1)^{(m-k)}\cdot\binom{m}{k}\cdot 2^k$$

$$1=(-1)^m+(-1)^{(m-1)}\cdot 2\mathrm{m}+\sum_{k=2}^{m}(-1)^{(m-k)}\cdot\binom{m}{k}\cdot 2^k$$

Which gives us:

$$2\cdot m=\sum_{k=2}^{m}(-1)^{(m-k)}\cdot\binom{m}{k}\cdot 2^k$$ for even m, m > 1, and

$$2-2\cdot m=\sum_{k=2}^{m}(-1)^{(m-k)}\cdot\binom{m}{k}\cdot 2^k$$ for odd m, m > 1

Dividing through by 4 in each case, we get:

$$\frac{m}{2}=\sum_{k=2}^{m}(-1)^{m-k}\cdot\binom{m}{k}\cdot 2^{k-2}$$ for even m, m > 1, and

$$\frac{1-m}{2}=\sum_{k=2}^{m}(-1)^{m-k}\cdot\binom{m}{k}\cdot 2^{k-2}$$ for odd m, m > 1

Now let n = m – 1. This yields:

$$\frac{n+1}{2}=\sum_{k=2}^{n+1}(-1)^{n+1-k}\cdot\binom{n+1}{k}\cdot 2^{k-2}$$ for odd n, n > 0, and

$$-\frac{n}{2}=\sum_{k=2}^{n+1}(-1)^{n+1-k}\cdot\binom{n+1}{k}\cdot 2^{k-2}$$ for even n, n > 0

The summation in these equations resemble that in what I called formula (ii) above:

(ii) $$a(n)=(-1)^n+\sum_{k=2}^{n+1}(-1)^{n+1-k}\cdot\binom{n+1}{k}\cdot(n+1)^{k-2}$$ for n > 0

Since we are going to be looking at congruences mod n–1, we can replace the final instance of “n+1” in that formula by “2”. After that we substitute in the identities we proved involving summations of binomial coefficients times the powers of 2:

$$a(n)\equiv(-1)^n+\sum_{k=2}^{n+1}(-1)^{n+1-k}\cdot\binom{n+1}{k}\cdot 2^{k-2}$$ (mod n–1) for n > 2

$$a(n)\equiv(-1)+\frac{n+1}{2}$$ (mod n–1) for odd n, n > 2

$a(n) \equiv (1) - \frac{n}{2}$ (mod n–1) for even n, n > 2

The congruence for odd n gives us exactly what we need:
a(n) ≡ (n–1)/2 = floor(n/2) (mod n–1).

In the congruence for even n, we just need to add (n–1) to the right-hand side, and we get a(n) ≡ n/2 = floor(n/2) (mod n–1).

Since 0 ≤ floor(n/2) < n, we have a(n) mod (n–1) = floor(n/2) for n > 2.

Q.E.D.

This is a special case of Theorem XII, below, which says:
For odd k:
a(km) ≡ (–1)^m (mod m)
a(km+1) ≡ ceiling(m/2) (mod m)
a(km–1) ≡ m/2 – 1 (mod m) for m even
a(km–1) ≡ 1 (mod m) for m odd

Setting k=1 and m=n–1, leads to a(n) ≡ floor(n/2) (mod n–1).

It follows that for m even, ½m divides a(m+1),
i.e. for all m, m divides a(2m+1).

And for m odd, m divides a(m+1) – ceiling(m/2)
so ½(m+1) divides a(m+1)–1
i.e. for all m, m divides a(2m)–1

IV. 4m divides a(2m)–1 for all m.

Up to now, I've shown several results involving the sequence A081215 mod m; we can in some cases strengthen the results by considering different expressions mod 4m.

For example, I previously showed: for all m, m divides a(2m)–1. Note: when I use the verb "divides" in this sense, I am defining it so that "0 divides 0" is true but "0 divides n" for any nonzero n is false. In other words, I am defining "a divides b", for any integers a and b, to mean "b is an integer multiple of a" (see https://math.stackexchange.com/q/666103).

It turns out that 4m divides a(2m)–1 for all m.

a(2m) = ((2m)^(2m+1) + 1) / (2m+1)^2

$(2m+1)^2 * a(2m) = (2m)^{(2m+1)} + 1$
$(4m^2 + 4m + 1) * a(2m) \equiv 2m*(2m)^{(2m)} + 1 \pmod{4m}$
$a(2m) \equiv 2m*(4m^2)^m + 1 \pmod{4m}$
$a(2m) \equiv 1 \pmod{4m}$
So 4m divides a(2m)–1.

What is a(2m+1) mod 4m ?
Conjecture: a(2m+1) mod 4m = m for m>0.
[Verified up to m = 5000.]

What is a(2m-1) mod 4m ?
Conjecture: for odd m, a(2m-1) mod 4m = m–1;
for even m, a(2m-1) mod 4m = 3m–1 (m>0).
[Verified up to m = 5000.]

What is a(2m) mod 3m ?
Conjecture: for m ≡ 1 (mod 3), a(2m) mod 3m = 1;
for m ≡ 0 or 2 (mod 3), a(2m) mod 3m = 2m+1 (m>0).
[Verified up to m = 5000.]

What is a(3m) mod 2m ?
Conjecture: for m mod 4 = 1, a(3m) mod 2m = 2m-1;
for m mod 4 = 3, a(3m) mod 2m = m-1;
for even m, a(3m) mod 2m = 1 (m>0).
[Verified up to m = 5000.]

```
What is a(7m) mod 6m ?
Conjecture: for m mod 12 = 0, a(7m) mod 6m = 4m+1; (m>0)
            for m mod 12 = 1, a(7m) mod 6m = 4m-1;
            for m mod 12 = 2, a(7m) mod 6m =    1;
            for m mod 12 = 3, a(7m) mod 6m = 5m-1;
            for m mod 12 = 4, a(7m) mod 6m = 4m+1;
            for m mod 12 = 5, a(7m) mod 6m = 6m–1;
            for m mod 12 = 6, a(7m) mod 6m = 4m+1;
            for m mod 12 = 7, a(7m) mod 6m =  m-1;
            for m mod 12 = 8, a(7m) mod 6m =    1;
            for m mod 12 = 9, a(7m) mod 6m = 2m-1;
            for m mod 12 =10, a(7m) mod 6m = 4m+1; and
            for m mod 12 =11, a(7m) mod 6m = 3m-1.
[Verified up to m = 5000.]
```

a(n) expressed in base n

V. In base n, a(n) has n-1 digits, which are (beginning from the left): n-2, 2, n-4, 4, n-6, 6, and so on, except that if n is even the rightmost digit is 1 instead of 0. In that case, the other digits form a palindrome with every even digit from 2 to n-2 appearing twice. For example, a(14) in base 14 is c2a486684a2c1. If n is odd, then all digits from 1 to n-1 occur exactly once (with n-1 as the rightmost digit). For example, a(15) in base 15 is d2b496785a3c1e.

The claim is that, for example,

$a(7) = 5*7^5 + 2*7^4 + 3*7^3 + 4*7^2 + 1*7^1 + 6*7^0$
$a(8) = 6*8^6 + 2*8^5 + 4*8^4 + 4*8^3 + 2*8^2 + 6*8^1 + 0*8^0 + 8*8^{-1}$

we could write, for any n>1,
a(n) = Sum_{k=1..floor(n/2)} $((n-2k)*n^{n-2k} + (2k)*n^{n-1-2k})$,
or equivalently,
a(n) = Sum_{k=1..floor(n/2)} $n^{n-2k} * (2k/n + n - 2k)$

and in the case of odd n > 1, say n=2m+1 and:

$$a(2m+1) = \sum_{k=1}^{m} 2k\cdot(2m+1)^{2m-2k} + \sum_{k=1}^{m} (2k-1)\cdot(2m+1)^{2k-1}$$

For example, a(13) = 20088655029078, which in base 13 is:

b29476583a1c, which is a permutation of 123456789abc: specifically, the permutation where the even digits stay where they are, while the odd digits appear in reverse order.

Now consider even n > 2. If n=2m:

$$a(2m) = 1 + \sum_{k=1}^{m-1} 2k\cdot(2m)^{2k} + \sum_{k=1}^{m-1} 2k\cdot(2m)^{2m-2k-1}$$

For example a(12) = 633095889817, which in base 12 is: a28466482a1. This is the palindrome a28466482a appended to 1.

An alternative way of writing this formula is to say n = 2m, and then for any even n >= 4:

$$a(n) = 1 + \sum_{k=1}^{\frac{n}{2}-1} 2\mathrm{k}\cdot\left(n^{2\mathrm{k}} + n^{n-1-2\mathrm{k}}\right)$$

Discussion:

This observation was motivated by a comment at
http://oeis.org/A060073

$A060073(n) = (n^{(n-1)} - 1) / (n-1)^2$

The comment states: “Written in base n, a(n) has n-2 digits and looks like 12345... except that the final digit is n-1 rather than n-2.”

Also, consider the relationship between A081215 and A081209. We have: A081209(n) = (n+1)*A081215(n). Now look at the table of each sequence in base n (for n=2 through n=33):

n	A081209(n) base n	A081215(n) base n
2	11	1
3	202	12
4	3031	221
5	40404	3214
6	505051	42241
7	6060606	523416
8	70707071	6244261
9	808080808	72543618
10	9090909091	826446281
11	a0a0a0a0a0a	927456381a
12	b0b0b0b0b0b1	a28466482a1
13	c0c0c0c0c0c0c	b29476583a1c
14	d0d0d0d0d0d0d1	c2a486684a2c1
15	e0e0e0e0e0e0e0e	d2b496785a3c1e
16	f0f0f0f0f0f0f0f1	e2c4a6886a4c2e1
17	g0g0g0g0g0g0g0g0g	f2d4b6987a5c3e1g
18	h0h0h0h0h0h0h0h0h1	g2e4c6a88a6c4e2g1
19	i0i0i0i0i0i0i0i0i0i	h2f4d6b89a7c5e3g1i
20	j0j0j0j0j0j0j0j0j0j1	i2g4e6c8aa8c6e4g2i1
21	k0k0k0k0k0k0k0k0k0k0k	j2h4f6d8ba9c7e5g3i1k
22	l0l0l0l0l0l0l0l0l0l0l1	k2i4g6e8caac8e6g4i2k1
23	m0m0m0m0m0m0m0m0m0m0m0m	l2j4h6f8dabc9e7g5i3k1m
24	n0n0n0n0n0n0n0n0n0n0n0n1	m2k4i6g8eaccae8g6i4k2m1
25	o0o0o0o0o0o0o0o0o0o0o0o0o	n2l4j6h8fadcbe9g7i5k3m1o
26	p0p0p0p0p0p0p0p0p0p0p0p0p1	o2m4k6i8gaecceag8i6k4m2o1
27	q0q0q0q0q0q0q0q0q0q0q0q0q0q	p2n4l6j8hafcdebg9i7k5m3o1q
28	r0r0r0r0r0r0r0r0r0r0r0r0r0r1	q2o4m6k8iagceecgai8k6m4o2q1
29	s0s0s0s0s0s0s0s0s0s0s0s0s0s0s	r2p4n6l8jahcfedgbi9k7m5o3q1s
30	t0t0t0t0t0t0t0t0t0t0t0t0t0t0t1	s2q4o6m8kaicgeegciak8m6o4q2s1

31	u0u0u0u0u0u0u0u0u0u0u0u0u0u0u0u0u	t2r4p6n8lajchefgdibk9m7o5q3s1u
32	v0v0v0v0v0v0v0v0v0v0v0v0v0v0v0v0v1	u2s4q6o8makcieggeickam8o6q4s2u1
33	w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w	v2t4r6p8nalcjehgfidkbm9o7q5s3u1w

Proof:

Maybe there’s a quicker way to prove this, but I’m just going to do the arithmetic in base n to show that these patterns continue, for both A081209 and A081215. The steps will be as follows:

First prove that A081209, which is defined as

A081209(n) = Sum_{k=0..n} $(-1)^{(n-k)}*n^k$,

is equal to $(n^{(n+1)}+(-1)^n) / (n+1)$
(this formula already appears at http://oeis.org/A081209).

Second, prove that the apparent pattern for A081209 in base n, as given in the table above, when multiplied by n+1 (which in base n is 11_n), gives the product $n^{n+1} + 1$ for n even and $n^{n+1} - 1$ for n odd.

Third, prove that the apparent pattern for A081215 in base n, as given in the table above, when multiplied by n+1, gives as product the pattern for A081209.

Step 1.
To prove: Sum_{k=0..n} $(-1)^{(n-k)}*n^k = (n^{(n+1)}+(-1)^n) / (n+1)$

Proof: multiply the left side by the denominator of the right side.

$$(n+1) * \sum_{k=0}^{n} (-1)^{n-k} \cdot n^k$$

$$= n \cdot \sum_{k=0}^{n} (-1)^{n-k} \cdot n^k + \sum_{k=0}^{n} (-1)^{n-k} \cdot n^k$$

$$= \sum_{k=0}^{n} (-1)^{n-k} \cdot n^{k+1} + \sum_{k=0}^{n} (-1)^{n-k} \cdot n^k$$

$$= \sum_{k=1}^{n+1} (-1)^{n-k+1} \cdot n^k + \sum_{k=0}^{n} (-1)^{n-k} \cdot n^k$$

$= (-1)^0 * n^{n+1} + (-1)^n * n^0$
$= n^{(n+1)} + (-1)^n$

Since the left side times the denominator of the right side equals the numerator of the right side, the left side equals the right side.

Step 2.

The pattern suggests that in base n, A081209(n) has n digits, with the first, third, fifth, and odd-positioned digits being n-1, and the second, fourth, sixth, and even-positioned digits being 0, except that if n is even, the nth digit is 1 instead of 0. We could write this as:

For n even, $1+(n-1)\cdot\sum_{k=0}^{\frac{n}{2}-1} n^{2k+1}$ (n > 0);

for n odd, $(n-1)\cdot\sum_{k=0}^{½(n-1)} n^{2k}$

Or we could merge these two formulas, and just write:

A081209(n) = (1 – n mod 2) + (n–1)* $\sum_{k=1}^{ceiling(n/2)} n^{n+1-2\cdot k}$ (n > 0)

But it's probably simpler to use the following formulation:

For n even, $1+(n-1)\cdot\sum_{k=1,3,5,\ldots,n-1} n^k$;

for n odd, $(n-1)\cdot\sum_{k=0,2,4,\ldots,n-1} n^k$

We are just taking the base-n formulation of a number and expressing it as a polynomial (evaluated at n). As examples, for n=6 we have $505051_6 = 1 + 5*(n^1 + n^3 + n^5)$, and for n=7 we have $6060606_7 = 6*(n^0 + n^2 + n^4 + n^6)$.

Now we are going to multiply by (n+1). We use the identity $(n+1)*(n-1) = n^2 - 1$. Thus the products are:

For n even, $(n+1)+(n^2-1)\cdot\sum_{k=1,3,5,\ldots,n-1} n^k$

$= \quad (n+1)+(\sum_{k=1,3,5,\ldots,n-1} n^{k+2})-(\sum_{k=1,3,5,\ldots,n-1} n^k)$

$= \quad (n+1)+(\sum_{k=3,5,7,\ldots,n+1} n^{k})-(\sum_{k=1,3,5,\ldots,n-1} n^k)$

$= \quad (n+1)+(n^{n+1})-(n^1) \quad = n^{n+1} + 1.$

And for n odd, $(n^2-1)\cdot\sum_{k=0,2,4,\ldots,n-1} n^k$

$= \quad (\sum_{k=0,2,4,\ldots,n-1} n^{k+2})-(\sum_{k=0,2,4,\ldots,n-1} n^k)$

$= \quad (\sum_{k=2,4,6,\ldots,n+1} n^{k})-(\sum_{k=0,2,4,\ldots,n-1} n^k)$

$= \quad (n^{n+1})-(n^0) \quad = n^{n+1} - 1.$

Since for both n even and n odd we've shown that (n+1) multiplied by this formulation is $n^{n+1} + (-1)^n$, then combining step 1 and step 2 we have now shown:

For n even (n ≠ 0), A081209(n) = $1+(n-1)\cdot\sum_{k=1,3,5,\ldots,n-1} n^k$; and

for n odd, A081209(n) = $(n-1)\cdot\sum_{k=0,2,4,\ldots,n-1} n^k$.

Step 3.

We want to prove that A081215(n) in base n satisfies the pattern observed in the table above, as examples: for n=8 6244261_8, and for n=9 72543618_9. We formulated this pattern above as:

For n even (n >= 4), a(n) = 1 + $\sum_{k=1}^{\frac{n}{2}-1} 2\mathrm{k}\cdot(n^{2\mathrm{k}}+n^{n-1-2\mathrm{k}})$;

for n odd (n >= 3), a(n) = $\sum_{k=1}^{½(n-1)} (2\mathrm{k}\cdot n^{n-1-2\mathrm{k}}+(2\mathrm{k}-1)\cdot n^{2\mathrm{k}-1})$.

But it's more convenient to formulate it analogously to the formulation in step 2, where we think of a number in base n as a polynomial evaluated at n that expressly shows the coefficient of n^k. Thus now we seek to prove the following:

For n even (n >= 4),
A081215(n) = $1 + \left(\sum_{k=2,4,6,\ldots,n-2} k\cdot n^k\right) + \left(\sum_{k=1,3,5,\ldots,n-3} (n-1-k)\cdot n^k\right)$;

for n odd (n >= 3),

A081215(n) = $\left(\sum_{k=0,2,4,\ldots,n-3} (n-1-k)\cdot n^k\right) + \left(\sum_{k=1,3,5,\ldots,n-2} k\cdot n^k\right)$.

And just to continue the examples I used above, for n=8 the formulation is

$6244261_8 = 1 + (2n^2 + 4n^4 + 6n^6) + (6n^1 + 4n^3 + 2n^5)$

and for n=9,

$72543618_9 = (8n^0 + 6n^2 + 4n^4 + 2n^6) + (1n^1 + 3n^3 + 5n^5 + 7n^7)$.

We have A081209(n) = $(n^{(n+1)}+(-1)^n) / (n+1)$ and
A081215(n) = $(n^{(n+1)}+(-1)^n) / (n+1)^2$ so therefore
A081215(n) = A081209(n) / (n+1).

So what we will do now is multiply our proposed formulation for A081215(n) by (n+1), and show that the product is the formulation of A081209(n) that we proved in step 2.

For n even (n >= 4),

$$(n+1) * \left(1 + \left(\sum_{k=2,4,6,\ldots,n-2} k\cdot n^k\right) + \left(\sum_{k=1,3,5,\ldots,n-3} (n-1-k)\cdot n^k\right)\right)$$

$$=\left(n + n*\sum_{k=2,4,6,\ldots,n-2} k\cdot n^k + n*\sum_{k=1,3,5,\ldots,n-3} (n-1-k)\cdot n^k\right) +$$
$$\left(1 + \sum_{k=2,4,6,\ldots,n-2} k\cdot n^k + \sum_{k=1,3,5,\ldots,n-3} (n-1-k)\cdot n^k\right)$$

$$=n + \sum_{k=2,4,6,\ldots,n-2} k\cdot n^{k+1} + \sum_{k=1,3,5,\ldots,n-3} (n-1-k)\cdot n^{k+1} +$$
$$1 + \sum_{k=2,4,6,\ldots,n-2} k\cdot n^k + \sum_{k=1,3,5,\ldots,n-3} (n-1-k)\cdot n^k$$

$$=n + \sum_{k=3,5,7,\ldots,n-1} (k-1)\cdot n^k + \sum_{k=2,4,6,\ldots,n-2} (n-k)\cdot n^k +$$
$$1 + \sum_{k=2,4,6,\ldots,n-2} k\cdot n^k + \sum_{k=1,3,5,\ldots,n-3} (n-1-k)\cdot n^k$$

$= n + (n-2)n^{n-1} + \sum_{k=3,5,7,\dots,n-3} (n-2)\cdot n^k + \sum_{k=2,4,6,\dots,n-2} n\cdot n^k +$

$1 + (n-2)n^1$

$= \sum_{k=3,5,7,\dots,n-1} (n-2)\cdot n^k + \sum_{k=3,5,7,\dots,n-1} n^k +$

$1 + (n-1)n^1$

$= 1 + \sum_{k=3,5,7,\dots,n-1} (n-1)\cdot n^k + (n-1)n^1$

$= 1 + (n-1)\cdot \sum_{k=1,3,5,\dots,n-1} n^k$ = A081209(n) = $(n^{(n+1)}+(-1)^n) / (n+1)$.

For n odd (n >= 3),

$(n+1) * \left(\sum_{k=0,2,4,\dots,n-3} (n-1-k)\cdot n^k + \sum_{k=1,3,5,\dots,n-2} k\cdot n^k \right)$

$= n*\left(\sum_{k=0,2,4,\dots,n-3} (n-1-k)\cdot n^k + \sum_{k=1,3,5,\dots,n-2} k\cdot n^k \right) +$

$\left(\sum_{k=0,2,4,\dots,n-3} (n-1-k)\cdot n^k + \sum_{k=1,3,5,\dots,n-2} k\cdot n^k \right)$

$= \sum_{k=0,2,4,\dots,n-3} (n-1-k)\cdot n^{k+1} + \sum_{k=1,3,5,\dots,n-2} k\cdot n^{k+1} +$

$\sum_{k=0,2,4,\dots,n-3} (n-1-k)\cdot n^k + \sum_{k=1,3,5,\dots,n-2} k\cdot n^k$

$= \sum_{k=1,3,5,\dots,n-2} (n-k)\cdot n^k + \sum_{k=2,4,6,\dots,n-1} (k-1)\cdot n^k +$

$\sum_{k=0,2,4,\dots,n-3} (n-1-k)\cdot n^k + \sum_{k=1,3,5,\dots,n-2} k\cdot n^k$

$= \sum_{k=1,3,5,\dots,n-2} n\cdot n^k + (n-2)n^{n-1} + \sum_{k=2,4,6,\dots,n-3} (n-2)\cdot n^k + (n-1)n^0$

$= \sum_{k=2,4,6,\dots,n-1} n^k + \sum_{k=2,4,6,\dots,n-1} (n-2)\cdot n^k + (n-1)n^0$

$= (n-1) \sum_{k=0,4,6,\dots,n-1} n^k$ = A081209(n) = $(n^{(n+1)}+(-1)^n) / (n+1)$.

Q.E.D.

(The above proof was specified to apply for even n >= 4 and odd n >= 3, but we can also observe A081215(2) = 1, which in base 2 has 1 digit, namely 1.)

Therefore:

For n even ($n \neq 0$), let $Q(x)$ be the polynomial of degree $n-2$ where the coefficient of x^0 is 1, for even nonzero k the coefficient of x^k is k, and for odd k the coefficient of x^k is $n-1-k$. Then A081215(n) = Q(n).

For n odd ($n \neq 1$), let $Q(x)$ be the polynomial of degree $n-2$ where for even k the coefficient of n^k is $n-1-k$ and for odd k the coefficient of n^k is k. Then A081215(n) = Q(n).

Two conjectures concerning A081215(n) expressed in base $(n-1)$:

For n odd, the last two digits of a(n) in base n-1 are 0 and (n-1)/2

For n even, the last two digits of a(n) in base n-1 are (n-2)/2 and n/2.

VI. a(n) mod 12 =
0, if n mod 24 = 1
1, if n mod 24 = 0, 2, 6, 8, 12, 14, 18, or 20
2, if n mod 24 = 5 or 21
3, if n mod 24 = 7
5, if n mod 24 = 3, 4, 10, 11, 16, or 22
6, if n mod 24 = 13
8, if n mod 24 = 9 or 17
9, if n mod 24 = 19
11, if n mod 24 = 15 or 23

Corollaries:
No term of the sequence is congruent to 4, 7, or 10 (mod 12);
a(n+3) - a(n+10) == floor(n/2) (mod 6) for n >= -3;
a(n) - a(n+2) == n (mod 6) for n >= 0;
a(n-4) - a(n) == 2n (mod 12) for n >= 4.

In other words, I will prove the following:
Taken mod 12, the first 24 terms of the sequence are:
1, 0, 1, 5, 5, 2, 1, 3, 1, 8, 5, 5,
1, 6, 1, 11, 5, 8, 1, 9, 1, 2, 5, 11,
and then those elements repeat; i.e. a(n) ≡ a(n mod 24) (mod 12).

PROOF: We will consider n mod 3 and n mod 8, and calculate a(n) mod 3 and a(n) mod 4, from which a(n) mod 12 follows.

First suppose n is even. Then we can have n ≡ 0, 1, or –1 (mod 3).

(n+1)^2 * a(n) = n^(n+1) + 1 (since n is even).

If n ≡ 0 (mod 3) then we get
a(n) ≡ 1 (mod 3)
If n ≡ 1 (mod 3) then we get
4 * a(n) ≡ 1 + 1 (mod 3)
a(n) ≡ 2 (mod 3)

If n ≡ –1 (mod 3) then we use the following formula:

$$a(n)=(-1)^n+\sum_{k=0}^{n-3}(-1)^{(n+1-k)}*\binom{n+1}{k+2}*(n+1)^k \quad \text{for } n > 2$$

Since n+1 ≡ 0 (mod 3), the terms in the summation all reduce to

0 (mod 3) except for at k=0. This gives us (for n even and $n \equiv -1 \pmod 3$):

$$a(n) \equiv 1 - C(n+1, 2) \pmod 3$$

Now $C(n+1, 2) = n(n+1)/2$. And since n is even, and $n \equiv 2 \bmod 3$, $n/2 \equiv 1 \pmod 3$. So $C(n+1, 2) \equiv 1*(n+1) \equiv 1*0 = 0 \pmod 3$.

Therefore $a(n) \equiv 1 \pmod 3$.

Now we also want to find a(n) mod 4. We're still supposing n is even, so start with $n \equiv 0 \pmod 4$. Then

$$(n+1)^2 * a(n) = n^{(n+1)} + 1$$
$$a(n) \equiv 1 \pmod 4.$$

And if $n \equiv 2 \pmod 4$ then

$$9*a(n) \equiv 2^{(n+1)} + 1 \pmod 4$$
$$a(n) \equiv 0 + 1 \pmod 4 \text{ (assuming } n > 2)$$
$$a(n) \equiv 1 \pmod 4$$

So now we can calculate a(n) mod 12 for any even value of n:

If $n \equiv 0 \pmod 3$ and n is even, then $a(n) \equiv 1 \pmod 3$ and $a(n) \equiv 1 \pmod 4$ so $a(n) \equiv 1 \pmod{12}$.

If $n \equiv 1 \pmod 3$ and n is even, then $a(n) \equiv 2 \pmod 3$ and $a(n) \equiv 1 \pmod 4$ so $a(n) \equiv 5 \pmod{12}$.

If $n \equiv 2 \pmod 3$ and n is even, then $a(n) \equiv 1 \pmod 3$ and $a(n) \equiv 1 \pmod 4$ so $a(n) \equiv 1 \pmod{12}$.

These values, mapping n mod 3 to a(n) mod 12, for even n, will be entered into the chart, below.

Now we turn to odd values of n. We have:

$$(n+1)^2 * a(n) = n^{(n+1)} - 1$$

If $n \equiv 0 \pmod 3$, this gives:

$$a(n) \equiv 2 \pmod 3$$

If $n \equiv 1 \pmod 3$, this gives:

$$4 * a(n) \equiv 0 \pmod 3$$

a(n) ≡ 0 (mod 3)

If n ≡ 2 (mod 3), then use this formula:

$$a(n)=(-1)^n+\sum_{k=0}^{n-3}(-1)^{(n+1-k)}*\binom{n+1}{k+2}*(n+1)^k \quad \text{for } n > 2$$

Since n+1 ≡ 0 (mod 3), the terms in the summation all reduce to 0 (mod 3) except for at k=0. And recalling that n is now odd, we have:

a(n) ≡ –1 + C(n+1, 2)

Now C(n+1, 2) = n(n+1)/2 and since n+1 is even, and n+1 ≡ 0 (mod 3), (n+1)/2 ≡ 0 (mod 3). Therefore C(n+1, 2) ≡ 0 (mod 3) and therefore a(n) ≡ –1 ≡ 2 (mod 3).

Now let's look at a(n) mod 4 for odd values of n.

$$a(n)=(-1)^n+\sum_{k=0}^{n-3}(-1)^{(n+1-k)}*\binom{n+1}{k+2}*(n+1)^k \quad \text{for } n > 2$$

If n ≡ 1 (mod 4) then the terms in the summation for k ≥ 2 are all 0, considered mod 4. So we just need to worry about k=0 and k=1:

a(n) ≡ –1 + C(n+1, 2) – C(n+1, 3) * 2 + C(n+1, 4) * 4 (mod 4)

Consider C(n+1, 3)*2. Since n is odd, n+1 and n-1 are even. C(n+1, 3) = (n+1)*n*(n-1) / 3*2*1. Since two even numbers appear in the numerator, the numerator is divisible by 4, while the denominator is not. Therefore C(n+1, 3) is even, so C(n+1, 3) * 2 is 0 (mod 4).

The rightmost term, C(n+1, 4) * 4 also vanishes, as 4 ≡ 0 (mod 4). We are left with:

a(n) ≡ –1 + C(n+1, 2) (mod 4)

Now, C(n+1, 2) = n(n+1)/2. When n ≡ 1 (mod 4), (n+1)/2 can be either 1 or 3 (mod 4). Specifically, if n ≡ 1 (mod 8), then (n+1)/2 is either 1 or 5 (mod 8) while if n ≡ 5 (mod 8) then (n+1)/2 is either 3 or 7 (mod 8). Therefore, if n ≡ 1 (mod 8) then (n+1)/2 ≡ 1 (mod 4), so a(n) ≡ 0 (mod 4), and if n ≡ 5 (mod 8) then (n+1)/2 ≡ 3 (mod 4), so a(n) ≡ 2 (mod 4).

That takes care of the case n ≡ 1 (mod 4).

Now suppose n ≡ 3 (mod 4).

$$a(n)=(-1)^n+\sum_{k=0}^{n-3}(-1)^{(n+1-k)}*\binom{n+1}{k+2}*(n+1)^k \quad \text{for } n > 2$$

All terms in the summation for k ≥ 1 come to 0 (mod 4), so we only need worry about k=0, and we get:

a(n) = –1 + C(n+1, 2)

Now n ≡ 3 (mod 4) so n ≡ either 3 or 7 (mod 8).

If n ≡ 3 (mod 8), then (n+1)/2 ≡ 2 or 6 (mod 8), so n ≡ 2 (mod 4), and a(n) ≡ –1 + C(n+1, 2) ≡ –1 + 3*2 ≡ 5 ≡ 1 (mod 4).

If n ≡ 7 (mod 8), then (n+1)/2 ≡ 0 or 4 (mod 8), so n ≡ 0 (mod 4), and a(n) ≡ –1 + C(n+1, 2) ≡ –1 + 3*0 ≡ –1 ≡ 3 (mod 4).

Summary for n odd:
If n ≡ 0 (mod 3), a(n) ≡ 2 (mod 3).
If n ≡ 1 (mod 3), a(n) ≡ 0 (mod 3).
If n ≡ 2 (mod 3), a(n) ≡ 2 (mod 3).
If n ≡ 1 (mod 8), a(n) ≡ 0 (mod 4).
If n ≡ 3 (mod 8), a(n) ≡ 1 (mod 4).
If n ≡ 5 (mod 8), a(n) ≡ 2 (mod 4).
If n ≡ 7 (mod 8), a(n) ≡ 3 (mod 4).

Combining these findings with the findings earlier, for even n, we can now build a chart to show the mapping from n (mod 24) to a(n) (mod 12):

n mod 24	n mod 3	n mod 8	a(n) mod 3	a(n) mod 4	a(n) mod 12
0	0	0	1	1	1
1	1	1	0	0	0
2	2	2	1	1	1
3	0	3	2	1	5

n mod 24	n mod 3	n mod 8	a(n) mod 3	a(n) mod 4	a(n) mod 12
4	1	4	2	1	5
5	2	5	2	2	2
6	0	6	1	1	1
7	1	7	0	3	3
8	2	0	1	1	1
9	0	1	2	0	8
10	1	2	2	1	5
11	2	3	2	1	5
12	0	4	1	1	1
13	1	5	0	2	6
14	2	6	1	1	1
15	0	7	2	3	11
16	1	0	2	1	5
17	2	1	2	0	8
18	0	2	1	1	1
19	1	3	0	1	9
20	2	4	1	1	1
21	0	5	2	2	2
22	1	6	2	1	5
23	2	7	2	3	11

Now I have proved:
Taken mod 12, the first 24 terms of the sequence are:

1, 0, 1, 5, 5, 2, 1, 3, 1, 8, 5, 5,
1, 6, 1, 11, 5, 8, 1, 9, 1, 2, 5, 11,

and then those elements repeat; i.e. a(n) ≡ a(n mod 24) (mod 12).

Corollaries:

a(n+3) – a(n+10) ≡ floor(n/2) (mod 6) for n >= –3

PROOF: First notice that above I have arranged the first 24 terms of sequence A081215, taken mod 12, in two lines. If we now work mod 6, we can see that in each column, the two numbers are congruent (mod 6). For example, from the arrangement above we see that a(3) ≡ 5 (mod 12) and a(15) ≡ 11 (mod 12) which tells us that both a(3) and a(15) are congruent to 5 (mod 6). Similarly, we can see that for all n, a(n) ≡ a(n mod 12) (mod 6). Now, let's place in one row, a(n) mod 6 for n=3 through 14, and in a row beneath it, a(n) mod 6 for n=10 through 21:

5, 5, 2, 1, 3, 1, 2, 5, 5, 1, 0, 1
5, 5, 1, 0, 1, 5, 5, 2, 1, 3, 1, 2

and now subtract modulo 6:

0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5

and since we've established that, considered modulo 6, the sequence repeats itself with period 12, this proves that for all n >= -3, a(n+3) – a(n+10) ≡ floor(n/2) (mod 6).

a(n) – a(n+2) ≡ n (mod 6) for n >= 0.

Proof: Verify this identity from the above sequence of the values of a(n) taken mod 12, checking each of the first 24 values of n. For example, 1 – 1 ≡ 0 (mod 6); 0 – 5 ≡ 1 (mod 6).

a(n–4) – a(n) ≡ 2n (mod 12) for n >= 4.

Proof: Again, just verify this from the theorem above, for n=4 through n=28, and then since everything is repeating mod 12 it's true for all n >= 4.

The propositions below are conjectures; I haven't proved them so I won't call them "corollaries" but I've verified them for values of n up to 5000.

```
a(n) - a(n+8)      ==   4n (mod 24)  for n >= 0
a(n+2) – a(n+18)  ==   8n (mod 48)  for n >= 1
a(n+6) - a(n+38)  ==  16n (mod 96)  for n >= -3
a(n+8) - a(n+72)  ==  32n (mod 192) for n >= -5
a(n) - a(n+128)   ==  64n (mod 384) for n >= 3
a(n+8) - a(n+264) == 128n (mod 768) for n >= -1
```

This suggests a pattern: for any positive integer k, there is some j such that

$a(n+j) - a(n+j+2^{k+1}) \equiv 2^k n \pmod{6*2^k}$ for sufficiently large n
or to state this a bit less rigorously:
if we define the sequence $r_k(n) = a(n) - a(n+2^{k+1}) \bmod 6*2^k$, then after the first several terms, this sequence $r_k(n)$ repeats with period 6 as 0, 2^k, $2*2^k$, $3*2^k$, $4*2^k$, $5*2^k$.

For example, $r_3(n) = a(n) - a(n+16) \bmod 48$ is, beginning at n=0:
32, 40, 24, 8, 16, 24, 32, 40, 0, 8, 16, 24, 32, 40, 0, 8, 16, 24, 32, 40, 0, 8, 16, 24, 32, 40, ...

I'm not going to try to prove that however.

Here are some other conjectures, all verified for values of n up to 5000:

a(4n) + a(4n+2) == 58 (mod 64) for n >= 1
a(4n+1) + a(4n+3) == 5 (mod 8) for n >= 0
a(4n+2) + a(4n+4) == 2 (mod 32) for n >= 1
a(4n+3) + a(4n+5) == 7 (mod 8) for n >= 0

a(10n) == 1 (mod 40)
a(10n+4) == 1 (mod 40)
a(10n+6) == 33 (mod 40)

a(30n) == 1 (mod 120)
a(30n+4) == 41 (mod 120)
a(30n+16) == 113 (mod 120)

a(60n+2) == 1 (mod 120)
a(60n+4) == 41 (mod 120)
a(60n+6) == 73 (mod 120)
a(60n+8) == 49 (mod 120)

I imagine that most if not all of those could be proved without much difficulty.

VII. If p is an odd prime, h is a nonnegative integer, k is a positive integer, and j is an integer greater than or equal to –hp, then

$$a(hp^k + j) \equiv a(hp + j) \pmod p.$$

In other words, we're saying that we can solve a(n) mod p by rewriting n in the form $n = hp^k + j$ and then we get a(n) mod p = a(hp+j) mod p. This makes it feasible to find a(n) mod p for very large values of n.

Proof:

Suppose p is an odd prime, h is a nonnegative integer, k is a positive integer, and j is an integer greater than –hp, and let x = A081215(hp + j) mod p.

Therefore:

$$(hp + j + 1)^2 * x \equiv (hp+j)^{hp+j+1} + (-1)^{hp+j} \pmod p$$
$$(j + 1)^2 * x \equiv (j)^{hp+j+1} + (-1)^{hp+j} \pmod p$$

and applying Fermat's Little Theorem:

$$(j + 1)^2 * x \equiv j^h * j^{j+1} + (-1)^{hp+j} \pmod p$$
$$(j + 1)^2 * x \equiv j^{j+1+h} + (-1)^{hp+j} \pmod p$$

Now let $y = A081215(hp^k + j) \bmod p$

$$(hp^k + j + 1)^2 * y \equiv (hp^k+j)\hat{}(hp^k + j + 1) + (-1)\hat{}(hp^k + j) \pmod p$$
$$(j + 1)^2 * y \equiv j\hat{}(hp^k + j + 1) + (-1)\hat{}(hp^k + j) \pmod p$$
$$(j + 1)^2 * y \equiv j\hat{}(hp^k) * j^{j+1} + (-1)\hat{}(hp^k + j) \pmod p$$

Since $(hp^k + j)$ has the same parity as (hp + j), $(-1)\hat{}(hp^k + j) = (-1)\hat{}(hp + j)$. Therefore,

$$(j + 1)^2 * y \equiv j\hat{}(hp^k) * j^{j+1} + (-1)\hat{}(hp + j) \pmod p$$
$$(j + 1)^2 * y \equiv (j\hat{}p^k)\hat{}h * j^{j+1} + (-1)^{hp + j} \pmod p$$

We can use a generalization of Fermat's Little Theorem (https://math.stackexchange.com/q/701071) which says that for any prime p and positive integer k, $j\hat{}(p^k) \equiv j \pmod p$. Then we have:

$(j + 1)^2 * y \equiv j\text{^}h * j^{j+1} + (-1)^{hp + j} \pmod p$
$(j + 1)^2 * y \equiv j^{j+1+h} + (-1)^{hp + j} \equiv (j + 1)^2 * x \pmod p$

If j+1 is not a multiple of p, then we can divide both sides of the congruence by $(j+1)^2$ to get $y \equiv x \pmod p$ which is what we set out to prove.

Now assume (j+1) is a multiple of p, say (j+1) = pz for some integer z. Then j = pz – 1. If $n = hp^k + j = hp^k + pz - 1$, then n+1 is a multiple of p.

Apply the formula:

$$\text{A081215}(n) = (-1)^n + \sum_{i=0}^{n-3} (-1)^{(n+1-i)} * \binom{n+1}{i+2} * (n+1)^i \quad \text{for } n > 2$$

Since (n+1) is a multiple of p, when we look at a congruence mod p, every term in the summation vanishes except for the term at i=0. This gives us:

A081215(n) ≡
$(-1)^n + (-1)^{n+1} * C(n+1, 2) \pmod p$

But since p is an odd prime, and n+1 is a multiple of p, C(n+1, 2) is a multiple of p. Then we have, for $n = hp^k + j$,

$\text{A081215}(n) \equiv (-1)^n \pmod p$

Recall that k is a positive integer and p is odd so $hp^k + j$ has the same parity as hp+j. This gives us:

$a(hp^k + j) \equiv (-1)^{hp+j} \equiv a(hp + j) \pmod p$

So now we are done. We’ve proved that $a(hp^k + j) \equiv a(hp + j) \pmod p$ in the two separate cases, first where j+1 is not a multiple of p and second where j+1 is a multiple of p.

As a side note, if we remove the requirement that p be prime, and instead of “p” refer to the variable as “m”, there are other cases where $a(hm^k + j) \equiv a(hm + j) \pmod m$, where m is composite, h and j are certain integers, and k is any positive integer. For example, considering $a(3*15^k + 20)$, that turns out to be congruent to –1 for k = 1, 2, 3, 4, and 5. I suspect for any positive integer k. That might not be hard to prove. Now replacing the “20” in that expression by 23, we get the following:

$a(3*15^1 + 23) \bmod 15 = 4$
$a(3*15^2 + 23) \bmod 15 = 13$
$a(3*15^3 + 23) \bmod 15 = 4$
$a(3*15^4 + 23) \bmod 15 = 13$
$a(3*15^5 + 23) \bmod 15 = 4$
$a(3*15^6 + 23) \bmod 15 = 13$

So one might speculate that for these values of h, m, and j, $a(hm^k + j) \bmod m$ is 4 for all odd values of k, and 13 for all even values of k.

Anyway I am not going to explore this.

VIII. For any odd prime p, and any positive integer k, at least one of the following is true: p divides k, p divides k+1, p divides a(kp–k–1).

Example: Take p=7 and k=8 through 12. The following terms of A081215 are divisible by 7: a(47), a(53), a(59), a(65), and a(71), but not a(77) or a(83).

Suppose k is a positive integer and p is an odd prime that divides neither k nor k+1. Set n=kp–k–1. Since p is odd, p–1 is even, so n = kp–k–1 = k(p–1)–1 is odd. Now, from the definition of a(n),

(kp–k)^2 * a(kp–k–1) = (kp–k–1)^(kp–k) – 1

(–k)^2 * a(kp–k–1) ≡ (–k–1)^(kp–k) – 1 (mod p)

k^2 * a(kp–k–1) ≡ $((-k-1)^{p-1})^k$ – 1 (mod p)

Since p does not divide k+1, p also does not divide -(k+1) = -k-1, so by Fermat’s Little Theorem, (–k–1)^(p–1) ≡ 1 (mod p). Then:

k^2 * a(kp–k–1) ≡ (1)^k – 1 (mod p)

k^2 * a(kp–k–1) ≡ 0 (mod p)

And since p does not divide k, we can divide by k^2 to get a(kp–k–1) ≡ 0 (mod p).

Now I have shown that if p divides neither k nor k+1, then p divides a(kp–k–1). I suspect the converse is also true: if p divides either k or k+1, then p does not divide a(kp–k–1). But I have not proved that. All I can say is, at least one of the following statements is true:
p divides k;
p divides k+1;
p divides a(kp–k–1).

Comment: since kp–k–1 = k(p–1)–1, if we look at a list of the prime factorizations of a(n) we will see that every (p–1)th term is divisible by p, beginning with (p–2), but excepting the following: (p-2)+(p-2)*(p-1), (p-2)+(p-1)*(p-1), and so forth. But there are many other terms of a(n), not caught by this

rule, that also are divisible by p. For example, take p=13. Then by this rule, we have the following divisible by p: a(11), a(23), a(35), a(47), a(59), a(71), a(83), a(95), a(107), a(119), and a(131), but not a(153) or a(165).
However, those are just 11 of the 24 terms of the sequence less than a(132) that are divisible by 13. Also it is interesting that even though a(153) and a(165) are not divisible by 13, a(151), a(157), a(167), and a(173) all are divisible by 13.

Now consider a larger prime, 647. Consider all the terms of the sequence that are divisible by 647, less than a(2000): a(1), a(67), a(322), a(360), a(594), a(645), a(849), a(985), a(1019), a(1025), a(1139), a(1291), a(1295), a(1614), a(1648), and a(1937).

Of those 16 terms, three are given by the pk-p-1 rule, namely: a(645), a(1291), and a(1937). Also, a(1295) is predicted by a different rule I proved, that a(2m+1) is divisible by m for all positive integers m. We note that a(322) is in the list, which is striking because 322 is close to half of 647 (647 = 2*322+3). Is there some general rule that a(m) is divisible by 2m+3?

For prime p, it is quite common to see a((p-3)/2) divisible by p. For example: 5 divides a(1); 19 divides a(8); 23 divides a(10); and 29 divides a(13). But there are many counterexamples too: 7 does not divide a(2), 11 does not divide a(4), 13 does not divide a(5), 17 does not divide a(7), and 31 does not divide a(14).

Of the integers q that divide a((q-3)/2), it appears that the vast majority but not all are prime, at least for values of q less than 4000. Here is a list of the 252 odd numbers q, less than 4000, satisfying q divides a((q-3)/2):
5, 19, 23, 29, 43, 47, 53, 65, 67, 71, 73, 97, 101, 133, 139, 149, 163, 167, 173, 191, 193, 197, 211, 239, 241, 263, 269, 283, 293, 307, 311, 313, 317, 331, 337, 359, 379, 383, 389, 409, 431, 433, 457, 461, 479, 499, 503, 509, 523, 529, 547, 557, 571, 577, 599, 601, 619, 643, 647, 653, 673, 677, 691, 701, 719, 739, 743, 769, 773, 787, 793, 797, 811, 821, 839, 859, 863, 883, 887, 907, 911, 937, 941, 983, 1009, 1013, 1031, 1033, 1051, 1061, 1103, 1109, 1123, 1129, 1151, 1153, 1171, 1181, 1201, 1223, 1229, 1249, 1277, 1291, 1297, 1301, 1319, 1321, 1367, 1373, 1439, 1459, 1483, 1487, 1489, 1493, 1511,

1531, 1559, 1579, 1583, 1607, 1609, 1613, 1627, 1637, 1657,
1699, 1709, 1723, 1729, 1733, 1747, 1753, 1777, 1801, 1823,
1847, 1867, 1871, 1873, 1877, 1901, 1949, 1973, 1987, 1993,
1997, 2011, 2017, 2039, 2059, 2063, 2069, 2083, 2087, 2089,
2111, 2113, 2131, 2137, 2141, 2161, 2179, 2203, 2207, 2213,
2237, 2251, 2281, 2309, 2321, 2333, 2347, 2351, 2357, 2371,
2377, 2381, 2399, 2423, 2447, 2465, 2467, 2473, 2477, 2521,
2539, 2543, 2549, 2591, 2593, 2617, 2621, 2659, 2663, 2683,
2687, 2689, 2693, 2707, 2711, 2713, 2731, 2741, 2789, 2803,
2833, 2837, 2851, 2857, 2861, 2879, 2903, 2909, 2927, 2953,
2957, 2971, 2999, 3001, 3019, 3023, 3049, 3067, 3119, 3121,
3163, 3167, 3169, 3187, 3191, 3217, 3221, 3259, 3307, 3313,
3331, 3359, 3361, 3389, 3407, 3413, 3433, 3457, 3461, 3499,
3527, 3529, 3533, 3547, 3557, 3571, 3581, 3623, 3643, 3671,
3673, 3677, 3691, 3697, 3701, 3719, 3739, 3767, 3769, 3793,
3797, 3821, 3863, 3889, 3907, 3911, 3917, 3931, 3989.

From that list, the only composite numbers are:
65, 133, 529, 793, 1729, 2059, 2321, and 2465.

Just not sure what to make of that. Of the odd numbers less than 4000, only about 27% are prime, but of the odd numbers less than 4000 satisfying q divides a((q-3)/2), about 97% are prime.

IX. For any odd prime p, p divides a(p-2), a(2p+1), a(2p-2)+1. Indeed, p divides a(p^k-2), a(2kp+1), and a(2p^k-2)+1 for any positive integer k.

Example: Take p=7 and k=1 through 9. The following are divisible by 7: a(5), a(47), a(341), a(2399), a(16805), a(117647), a(823541), a(5764799), a(40353605), a(15), a(29), a(43), a(57), a(71), a(85), a(99), a(113), a(127), a(12)+1, a(96)+1, a(684)+1, a(4800)+1, a(33612)+1, a(235296)+1, a(1647084)+1, a(11529600)+1, a(80707212)+1.

Proof:

Suppose p is an odd prime and k is a positive integer. Since p is odd, $p^k - 2$ is odd so $(-1)^{(p^k - 2)} = -1$.

Now $a(p^k - 2) = ((p^k - 2)^{(p^k - 1)} - 1) / (p^k - 1)^2$

$$\therefore (p^k - 1)^2 * a(p^k - 2) = (p^k - 2)^{(p^k - 1)} - 1$$

$$(p^{(2k)} - 2(p^k) + 1) * a(p^k - 2) \equiv (p^k - 2)^{(p^k - 1)} - 1 \pmod p$$

$$1 * a(p^k - 2) \equiv (-2)^{(p^k - 1)} - 1 \pmod p$$

Because $p^k - 1$ is even, $(-2)^{(p^k - 1)} = 2^{(p^k - 1)}$.

$$a(p^k - 2) \equiv 2^{(p^k - 1)} - 1 \pmod p$$

Now multiply through by 2:

$$2 * a(p^k - 2) \equiv 2^{(p^k)} - 2 \pmod p$$

Now, consider the right-hand side of this congruence. Making use of the proofs at the following link:
https://math.stackexchange.com/q/701071

We have $2^{(p^k)} - 2 \equiv 0 \pmod p$

$\therefore 2 * a(p^k - 2) \equiv 0 \pmod p$
and since p is odd,
$a(p^k - 2) \equiv 0 \pmod p$
Q.E.D.
Note: the smallest *composite* number n that divides a(n-2) is n=341.

Now let k be any nonnegative integer, p an odd prime, and consider a(2kp+1) (mod p).

Since 2kp+1 is odd, (–1)^(2kp+1) = –1.

a(2kp+1) = ((2kp+1)^(2kp+2) – 1) / (2kp+2)^2

(2kp+2)^2 * a(2kp+1) ≡ (2kp+1)^(2kp+2) – 1 (mod p)

4 * a(2kp+1) ≡ (1)^(2kp+2) – 1 (mod p)

4 * a(2kp+1) ≡ 0 (mod p)

And since p is odd, a(2kp+1) ≡ 0 (mod p) Q.E.D.

Actually, I never used the fact that p is prime in that proof. Therefore, for any odd positive integer m,
a(2km+1) ≡ 0 (mod m).

That proof is valid where p is an odd prime, but the proposition also happens to be true that if p=2, p divides a(2kp+1), i.e. a(4k+1) is even for k = 0, 1, 2, 3, ... (This follows from something I proved in section III of this document, that for all m, m divides a(2m+1). Now for any k set m=2k and m divides a(4k+1), and since we've defined m here to be even, a(4k+1) is even.)

Here is another way of proving that a(4k+1) is even:

We have $a(n)=\frac{n^{n+1}+(-1)^n}{(n+1)^2}$

Take n=4k+1 and then since n mod 8 is either 1 or 5, the denominator, $(n+1)^2$, is divisible by 4 but not 8. Whereas the numerator,
n^(n+1) + (–1)^n, *is* divisible by 8. Therefore a(n) is even.

Therefore we have proved:
p divides a(p^k – 2) for any odd prime p and any positive integer k; and
p divides a(2kp+1) for any prime p and any nonnegative integer k.

$a(hp^k - 2)$ modulo p

X. For any prime p, and any positive integers k and h such that $h*p > 2$, $a(hp^k - 2) \equiv (1 - 2^{h-1})*(-1)^h \pmod{p}$. For example: $a(5p^k - 2) \equiv 15 \pmod{p}$; $a(10p^k - 2) \equiv -511 \pmod{p}$.

PROOF:

First suppose h is an even positive integer, and p is any prime.

$$(hp - 1)^2 * a(hp - 2) = (hp - 2)^{hp - 1} + (-1)^{hp - 2}$$

Since h is even, $(-1)^{hp - 2} = 1$. Therefore:

$$(hp - 1)^2 * a(hp - 2) \equiv (hp - 2)^{hp - 1} + 1 \pmod{p}$$
$$a(hp - 2) \equiv ((-2)^p)^h / (-2) + 1 \pmod{p}$$

Applying Fermat's Little Theorem:

$$a(hp - 2) \equiv (-2)^{(h-1)} + 1 \pmod{p}$$

And since h is even, $h - 1$ is odd, so we have

$$a(hp - 2) \equiv 1 - 2^{(h-1)} \pmod{p}$$

Now suppose h is an odd positive integer, and p is an odd prime.

$$(hp - 1)^2 * a(hp - 2) = (hp - 2)^{hp - 1} + (-1)^{hp - 2}$$

Since h and p are both odd, $(-1)^{hp - 2} = -1$. Therefore:

$$(hp - 1)^2 * a(hp - 2) \equiv (hp - 2)^{hp - 1} - 1 \pmod{p}$$
$$a(hp - 2) \equiv ((-2)^p)^h / (-2) - 1 \pmod{p}$$

Applying Fermat's Little Theorem:

$$a(hp - 2) \equiv (-2)^{(h-1)} - 1 \pmod{p}$$

And since h is odd, $h - 1$ is even, so we have

$$a(hp - 2) \equiv 2^{(h-1)} - 1 \pmod{p}$$

That proof made use of the supposition that p is odd. If p=2, we have, for any positive integer h and any positive integer k:

$$(hp^k - 1)^2 * a(hp^k - 2) \equiv (hp^k - 2)^{(hp^k - 1)} + (-1)^{hp^k} \pmod{p}$$
$$a(2^k h - 2) \equiv (0)^{(2^k h - 1)} + 1 \pmod{2}$$
$$a(2^k h - 2) \equiv 1 \pmod{2}.$$

Now if h=1 then $(-1)^h * (1 - 2^{h-1}) \equiv 0 \pmod{2}$ so the congruence does not hold. But if h is greater than 1, $(-1)^h * (1 - 2^{h-1})$ is odd, so $(-1)^h * (1 - 2^{h-1}) \equiv 1 \equiv a(2^k h - 2) \pmod{2}$.

So now I have proved, for any prime p and any positive integer h, other than the case p=2 and h=1:

$$a(hp - 2) \equiv (-1)^h * (1 - 2^{h-1}) \pmod{p}$$

And then by Theorem VII, we can say: for any prime p and any positive integers h and k,

$a(hp^k - 2) \equiv (-1)^h * (1 - 2^{h-1}) \pmod{p}$ unless p=2 and h=1.

Q.E.D.

$\underline{a(hp^k - 3) \text{ modulo } p}$

XI. For any prime p > 3 and any positive integer k,
if $p \equiv 1 \pmod 3$ then $a(p^k - 3) \equiv (1-p)/6 \pmod p$; and
if $p \equiv -1 \pmod 3$ then $a(p^k - 3) \equiv (1+p)/6 \pmod p$.
For any odd prime p, any positive integer k, and any odd integer h > 1, $a(hp^k - 3) \equiv (p+z)/2 \pmod p$, where $z = (9 - 3^h)/18$. For example, $a(5p^k - 3) \equiv (p - 13)/2 \pmod p$.
For any odd prime p, any positive integer k, and any positive even number h such that h*p > 6,
$a(hp^k - 3) \equiv (3^h - 9)/36 \pmod p$.
For example, $a(10p^k - 3) \equiv 1640 \pmod p$.

First look at the case h=5.
To prove: $a(5p-3) \equiv (p-13)/2 \pmod p$ for any odd prime p

$(5p-2)^2 * a(5p-3) = (5p-3)^{5p-2} + 1$
$4 * a(5p-3) \equiv -3^{5p-2} + 1 \pmod p$
$4 * a(5p-3) \equiv -3^{5p-2} + 1 \pmod p$
multiply through by 9:
$36*a(5p-3) \equiv -3^{5p} + 9 \pmod p$
$36*a(5p-3) \equiv -3^{5} + 9 \pmod p$ by Fermat's Little Theorem
$36*a(5p-3) \equiv -234 \pmod p$

Now suppose $p \neq 3$. Then gcd(p, 18) = 1 so we can divide through by 18:
$2*a(5p-3) \equiv -13 \pmod p$
Now, since p is odd, (p+1)/2 is an integer, so multiply through by that:
$(p+1)*a(5p-3) \equiv -13(p+1)/2 \pmod p$
$a(5p-3) \equiv -13(p+1)/2 \pmod p$
And we can add 7p to the right side, yielding:
$a(5p-3) \equiv 7p - (13(p+1)/2) \pmod p$
$a(5p-3) \equiv (p-13)/2 \pmod p$

Now at one step we supposed $p \neq 3$. So now let's check whether the congruence holds for p=3:
$a(5*3 - 3) = 633095889817 \equiv 1 \pmod 3$
$(3-13)/2 = -5 \equiv 1 \pmod 3$

Therefore we can now say $a(5p-3) \equiv (p-13)/2 \pmod p$ for any odd prime p. And from Theorem VII, above, we can say:
$a(5p^k - 3) \equiv (p-13)/2 \pmod p$ for any odd prime p and any positive integer k.

To prove:
For any prime $p > 3$ and any positive integer k,

if $p \equiv 1 \pmod 3$ then $a(p^k - 3) \equiv (1-p)/6 \pmod p$; and

if $p \equiv -1 \pmod 3$ then $a(p^k - 3) \equiv (1+p)/6 \pmod p$.

First we'll ignore the k (i.e. take $k=1$). Suppose p is a prime other than 2 or 3.

Now by the definition of $a(n)$,

$$(p-2)^2 * a(p-3) = (p-3)^{p-2} + (-1)^{p-3}$$

Since p is odd, $(-1)^{p-3} = 1$. Modulo p, we get:

$$(-2)^2 * a(p-3) \equiv (-3)^{p-2} + 1 \pmod p$$
$$4 * a(p-3) \equiv 1 - 3^{p-2} \pmod p$$

now multiply through by 9:

$$36 * a(p-3) \equiv 9 - 3^p \pmod p$$
$$36 * a(p-3) \equiv 6 \pmod p\text{, by Fermat's Little Theorem}$$

Since p is a prime other than 2 or 3, $\gcd(6, p) = 1$ and we can divide both sides of the congruence by 6:

$$6 * a(p-3) \equiv 1 \pmod p$$

Now p must be congruent to either 1 or $-1 \pmod 3$. First suppose $p \equiv 1 \pmod 3$. Then $1-p$ is divisible by 3, and since p is odd, $1-p$ is even so therefore $(1-p)/6$ is an integer. Now multiply both sides of the congruence by $(1-p)/6$:

$$(1-p) * a(p-3) \equiv (1-p)/6 \pmod p$$

But on the left side, we can replace $(1-p)$ by 1, giving us what we need:

$$a(p-3) \equiv (1-p)/6 \pmod p \text{ if } p \equiv 1 \pmod 3$$

Now suppose $p \equiv -1 \pmod 3$. Then $1+p$ is divisible by 3, and since p is odd, $1+p$ is even so therefore $(1+p)/6$ is an integer. Now go back to the congruence we had before and multiply both sides by $(1+p)/6$:

$$6 * a(p-3) \equiv 1 \pmod{p}$$
$$(1+p) * a(p-3) \equiv (1+p)/6 \pmod{p}$$
$$a(p-3) \equiv (1+p)/6 \pmod{p} \text{ if } p \equiv -1 \pmod{3}.$$

That proves our statement for the case k=1. Then by theorem VII (above in this document), the proposition generalizes to $a(p^k-3) \pmod{p}$ for any positive integer k. Q.E.D.

Now suppose p is any odd prime and h is any odd positive integer greater than 1.

$$(hp - 2)^2 * a(hp - 3) = (hp - 3)^{hp - 2} + (-1)^{hp - 3}$$

Since h and p are both odd, $(-1)^{hp - 3} = 1$. Therefore:

$$(hp - 2)^2 * a(hp - 3) \equiv (hp - 3)^{hp - 2} + 1 \pmod{p}$$
$$4 * a(hp - 3) \equiv (-3)^{hp - 2} + 1 \pmod{p}$$

Now multiply through by 9:

$$36 * a(hp - 3) \equiv (-3)^{hp} + 9 \pmod{p}$$
$$36 * a(hp - 3) \equiv ((-3)^p)^h + 9 \pmod{p}$$

Applying Fermat’s Little Theorem:
$$36 * a(hp - 3) \equiv (-3)^h + 9 \pmod{p}$$

Now let $y = (-3)^h + 9$ and think about the divisibility properties of y. Since h > 1, $(-3)^h + 9$ is divisible by 9. But what is y mod 4?

$$y = (-3)^h + 9 \equiv (1)^h + 1 = 2 \pmod{4}$$

Therefore y is divisible by 2 and 9 but not 4. Therefore we can write y = 18z where z is some odd integer (because if z were even, y mod 4 would be 0).

To recap, what we have so far is:

$$36 * a(hp - 3) \equiv (-3)^h + 9 = y = 18z \pmod{p}$$

Now let’s suppose p ≠ 3. Then (since p also ≠ 2), gcd(18, p) = 1 and we can divide both sides of the congruence by 18, giving us:

$$2 * a(hp - 3) \equiv z \pmod{p}$$

Now multiply both sides by (p+1)/2:

$$(p+1) * a(hp - 3) \equiv z(p+1)/2 \pmod{p}$$

Now of course the (p+1) on the left side is just 1 (mod p) and on the right side, since z is odd we can add p(1-z)/2:

$$a(hp - 3) \equiv p(1-z)/2 + z(p+1)/2 \pmod{p}$$
$$a(hp - 3) \equiv (p+z)/2 \pmod{p} \text{ where } z = (9 - 3^h)/18$$

Okay, what I've proved so far is that for p any prime greater than 3, and h an odd integer greater than 1, $a(hp - 3) \equiv (p+z)/2 \pmod{p}$ where $z = (9 - 3^h)/18$. For example:
$a(3p - 3) \equiv (p-1)/2 \pmod{p}$
$a(5p - 3) \equiv (p-13)/2 \pmod{p}$
$a(7p - 3) \equiv (p-121)/2 \pmod{p}$
$a(9p - 3) \equiv (p-1093)/2 \pmod{p}$

Now what if p=3? a(h*3 – 3) mod 3 = a((h-1)*3) mod 3 where h-1 is even. And I've already proved that $a(km) \equiv 1 \pmod{m}$ when k is even. Therefore, if p=3, $a(hp - 3) \equiv 1 \pmod{p}$. For the other side of the congruence,

$$\begin{aligned}(p+z)/2 &= (3 + ((9 - 3^h)/18))/2 \\ &= (54 + 9 - 3^h)/36 \\ &= (7 - 3^{h-2})/4 \text{ since h is greater than or equal to 3.}\end{aligned}$$

Therefore:

$$4 * (p+z)/2 \equiv 7 - 3^{h-2} \pmod{3}$$
$$(p+z)/2 \equiv 1 \pmod{3}$$

and that proves that for p=3 and h an odd integer greater than 1, $a(hp - 3) \equiv 1 \equiv (p+z)/2 \pmod{p}$ where $z = (9 - 3^h)/18$.

Then because of the other theorem I proved, we can stick an exponent k after the p, and we get:

For any odd prime p, and any odd integer h > 1, and any positive integer k,
$a(hp^k - 3) \equiv (p+z)/2 \pmod{p}$ where $z = (9 - 3^h)/18$.

Now what if h is an even positive integer, then what is a(hp – 3) (mod p)? Well if h is even then hp – 3 is odd, so we have:

$$(hp - 2)^2 * a(hp - 3) = (hp - 3)^{hp-2} - 1$$
$$4 * a(hp - 3) \equiv (-3)^{hp-2} - 1 \pmod p$$
$$4 * a(hp - 3) \equiv 3^{hp-2} - 1 \pmod p \text{ since h is even}$$

Multiply through by 9:
$$36 * a(hp - 3) \equiv 3^{hp} - 9 \pmod p$$
$$36 * a(hp - 3) \equiv 3^{h} - 9 \pmod p \text{ by Fermat's Little Theorem}$$

Now let $y = 3^h - 9$ and consider whether y is divisible by 4. Recalling that h is even, observe that $y \equiv 1 - 1 = 0 \pmod 4$. And since h is at least 2, y is divisible by 9. Thus y is divisible by 36, so say y = 36w for some integer w. And now
$$36 * a(hp - 3) \equiv 36w \pmod p$$

So let's suppose $p \neq 3$, and then since p is an odd prime, gcd(36, p) = 1 and we can say:
$a(hp - 3) \equiv w \pmod p$ where $w = (3^h - 9)/36$.

And what if p=3? Then for even h, let $w = (3^h - 9)/36$ and we hope to prove that $a(h*3 - 3) \equiv w \pmod 3$.

a(h*3 – 3) = a((h-1)*3) and h-1 is odd. But I've already proved that for k odd, a(km) == (-1)^m (mod m). This gives:
$a(h*3 - 3) \equiv -1 \pmod 3$.

Now for the right side, we need to prove $w \equiv -1 \pmod 3$.

Notice that $w + 1 = (3^h - 9 + 36)/36$
$= (3^h + 27)/36$

We know that h is even, and we can see that if h=2, w+1 = 1 so the congruence is not satisfied. But if h is an even number greater than 2, then the numerator is divisible by 27 and also divisible by 4 (since $3^h \equiv 1 \pmod 4$ for h even, and $27 \equiv 3 \pmod 4$). The denominator is equal to 9*4, so $w + 1 = (3^h + 27)/36$ is an integer divisible by 3. Hence $w \equiv -1 \pmod 3$ which is what we needed to prove.

We have found that if p is a prime greater than 3, h can be any positive even number, but if p=3 then h cannot be 2. That exception (i.e. for p=3 and h=2, $a(hp - 3) \not\equiv 3^h - 9 \pmod{p}$) is a special case of Theorem VIII, "if p is an odd prime that divides neither k nor k+1, then p divides $a(kp-k-1)$" (take k=2). That shows why it doesn't work for p=3.

Thus we've proved that for any odd prime p, and any positive even number h such that h*p > 6, $a(hp - 3) \equiv (3^h - 9)/36 \pmod{p}$. For example:
$a(2p - 3) \equiv 0 \pmod{p}$ (unless p=3)
$a(4p - 3) \equiv 2 \pmod{p}$
$a(6p - 3) \equiv 20 \pmod{p}$
$a(8p - 3) \equiv 182 \pmod{p}$
$a(10p - 3) \equiv 1640 \pmod{p}$
$a(12p - 3) \equiv 14762 \pmod{p}$

And also by Theorem VII we can stick in an exponent k like so:

For any odd prime p, any positive integer k, and any positive even number h such that h*p > 6, $a(hp^k - 3) \equiv (3^h - 9)/36 \pmod{p}$.

Q.E.D.

Recap, and further conjectures, about a(hp + j) (mod p) for odd prime p:

```
a(p-2) ≡ 0 (mod p)         Theorem IX; Theorem X.
a(p-1) ≡ 1 (mod p)         Theorem II.
a(p) ≡ -1 (mod p)          Theorem I.
a(p+1) ≡ (p+1)/2 (mod p)   Theorem III.
a(2p-3) ≡ 0 (mod p)        Theorem XI.
a(2p-2) ≡ -1 (mod p)       Theorem IX; Theorem X.
a(2p-1) ≡ -1 (mod p)       Theorem XII.
a(2p) ≡ 1 (mod p)          Theorem IV.
a(2p+1) ≡ 0 (mod p)        Theorem IX.
a(3p-4) ≡ 0 (mod p) (for p > 3)  Theorem VIII.
a(3p-3) ≡ (p-1)/2 (mod p) Theorem XI.
a(3p-2) ≡ 3 (mod p)        Theorem X.
a(3p-1) ≡ 1 (mod p)        Theorem XII.
a(3p) ≡ -1 (mod p)         Theorem XII.
a(3p+1) ≡ (p+1)/2 (mod p) Theorem XII.
a(3p+2) ≡ 7 (mod p) (for p > 3)  [conjectured]
a(4p-5) ≡ 0 (mod p) (for p > 5)  Theorem VIII.
a(4p-3) ≡ 2 (mod p)        Theorem XI.
a(4p-2) ≡ -7 (mod p)       Theorem X.
a(4p-1) ≡ -1 (mod p)       Theorem XII.
a(4p) ≡ 1 (mod p)          Theorem XII.
a(4p+1) ≡ 0 (mod p)        Theorem IX.
a(5p-6) ≡ 0 (mod p) (for p > 5)  Theorem VIII.
a(5p-3) ≡ (p-13)/2 (mod p) Theorem XI.
a(5p-2) ≡ 15 (mod p)       Theorem X.
a(5p-1) ≡ 1 (mod p)        Theorem XII.
a(5p) ≡ -1 (mod p)         Theorem XII.
a(5p+1) ≡ (p+1)/2 (mod p) Theorem XII.
a(6p-7) ≡ 0 (mod p) (for p > 7)  Theorem VIII.
a(6p-3) ≡ 20 (mod p)       Theorem XI.
a(6p-2) ≡ -31 (mod p)      Theorem X.
a(6p-1) ≡ -1 (mod p)       Theorem XII.
a(6p) ≡ 1 (mod p)          Theorem XII.
a(6p+1) ≡ 0 (mod p)        Theorem IX.
a(6p+2) ≡ 57 (mod p) (for p > 3) [conjectured]
a(7p-8) ≡ 0 (mod p) (for p > 7)  Theorem VIII.
a(7p-3) ≡ (p-121)/2 (mod p) Theorem XI.
a(7p-2) ≡ 63 (mod p)       Theorem X.
a(7p-1) ≡ 1 (mod p)        Theorem XII.
a(7p) ≡ -1 (mod p)         Theorem XII.
a(7p+1) ≡ (p+1)/2 (mod p) Theorem XII.
```

$a(8p-9) \equiv 0 \pmod{p}$ (for $p > 7$) Theorem VIII.
$a(8p-5) \equiv 39 \pmod{p}$ [conjectured] (seems to be true for all primes and many nonprimes, e.g. $a(8*65-5) \equiv 39 \pmod{65}$, $a(8*66-5) \equiv 39 \pmod{66}$.)
$a(8p-3) \equiv 182 \pmod{p}$ Theorem XI.
$a(8p-2) \equiv -127 \pmod{p}$ Theorem X. (also seems to be true for many, many nonprimes, e.g. $a(8*112-2) \equiv -127 \pmod{112}$)
$a(8p-1) \equiv -1 \pmod{p}$ Theorem XII.
$a(8p) \equiv 1 \pmod{p}$ Theorem XII.
$a(8p+1) \equiv 0 \pmod{p}$ Theorem IX.
$a(9p-10) \equiv 0 \pmod{p}$ (for $p > 5$) Theorem VIII.
$a(9p-7) \equiv (p-19)/2 \pmod{p}$ [conjectured]
$a(9p-3) \equiv (p-1093)/2 \pmod{p}$ Theorem XI.
$a(9p-2) \equiv 255 \pmod{p}$ Theorem X.
$a(9p-1) \equiv 1 \pmod{p}$ Theorem XII.
$a(9p) \equiv -1 \pmod{p}$ Theorem XII.
$a(9p+1) \equiv (p+1)/2 \pmod{p}$ Theorem XII.
$a(9p+2) \equiv 455 \pmod{p}$ [conjectured]
$a(10p-11) \equiv 0 \pmod{p}$ (for $p > 11$) Theorem VIII.
$a(10p-3) \equiv 1640 \pmod{p}$ Theorem XI.
$a(10p-2) \equiv -511 \pmod{p}$ Theorem X. (appears to be true for many nonprimes as well)

XII. Suppose k and m are positive integers. Then,
For even k:

$$a(km) \equiv 1 \pmod m$$
$$a(km+1) \equiv 0 \pmod m$$
$$a(km-1) \equiv -1 \pmod m$$

For odd k:

$$a(km) \equiv (-1)^m \pmod m$$
$$a(km+1) \equiv \lceil m/2 \rceil \pmod m$$
$$a(km-1) \equiv 1 \pmod m \text{ for } m \text{ odd}$$
$$a(km-1) \equiv m/2 - 1 \pmod m \text{ for } m \text{ even}$$

Proof:

We are going to prove a more consolidated version of these statements, namely for positive integers k and m:

$$a(km) \equiv (-1)^{km} \pmod m$$
$$a(km+1) \equiv \lceil km/2 \rceil \pmod m$$
For odd m, $a(km-1) \equiv (-1)^{k+1} \pmod m$
For even m, $a(km-1) \equiv (km/2) - 1 \pmod m$

Begin with:
$(n+1)^2 * a(n) \equiv n^{n+1} + (-1)^n \pmod m$ **[**]**

First take n=km. We want to prove $a(km) \equiv (-1)^{km} \pmod m$. This follows from the congruence **[**]**:

$$(km+1)^2 * a(km) \equiv (km)^{km+1} + (-1)^{km} \pmod m$$
$$1^2 * a(km) \equiv (0)^{km+1} + (-1)^{km} \pmod m$$
$$a(km) \equiv (-1)^{km} \pmod m$$

Therefore if k is even, $a(km) \equiv 1 \pmod m$; if k is odd, $a(km) \equiv (-1)^m \pmod m$.

Now take n=km+1. We want to prove $a(km+1) \equiv \lceil km/2 \rceil \pmod m$. Substituting into **[**]**:

$$(km+2)^2 * a(km+1) \equiv (km+1)^{km+2} + (-1)^{km+1} \pmod m$$
$$2^2 * a(km+1) \equiv (1)^{km+2} + (-1)^{km+1} \pmod m$$
$$4 * a(km+1) \equiv 0 \pmod m \text{ if } km \text{ is even, } 2 \pmod m \text{ if } km \text{ is odd}$$ **[***]**

Now we have to consider different cases, depending on whether k and m are odd or even.

If k and m are both odd, we have, from **[***]**:

$$4 * a(km+1) \equiv 2 \pmod{m}$$

We can divide both sides by 2 since m is odd:

$$2 * a(km+1) \equiv 1 \pmod{m}$$

Now multiply both sides by $\frac{1}{2}(m+1)$:

$$(m+1)*a(km+1) \equiv \tfrac{1}{2}(m+1) \pmod{m} \quad = \text{ceiling}(m/2)$$

Now the m+1 on the left-hand side is just 1 mod m, and on the right-hand side, we are going to add $\frac{1}{2}m(k-1)$, which is an integer divisible by m because k is odd. This yields:

$$a(km+1) \equiv \tfrac{1}{2}(m + 1 + km - m) \pmod{m}$$

$$a(km+1) \equiv \tfrac{1}{2}(km + 1) \pmod{m} = \text{ceiling}(km/2) \text{ for odd } k$$

and odd m.

If k is even and m is odd, we have, from **[***]**:

$$4 * a(km+1) \equiv 0 \pmod{m}$$

and we can divide both sides by 4 since m is odd, giving us

$$a(km+1) \equiv 0 \pmod{m}$$

Since k is even, ceiling(km/2) ≡ 0 (mod m) so we can write

$$a(km+1) \equiv \text{ceiling}(km/2) \pmod{m} \text{ for even } k \text{ and odd } m.$$

So far we’ve shown that a(km+1) ≡ ceiling(km/2) (mod m) for m odd.

Now suppose m is even, with n=km+1. Let q = $\frac{1}{2}$m.

(2kq+2)^2 * a(km+1) = (2kq+1)^(2kq+2) + (-1)^(km+1)

We are going to do our calculations mod 4m = 8q. Afterwards it will be easy to deduce a(km+1) (mod m) when we know a(km+1) (mod 4m). We know that km+1 is odd, so
$(-1)^{km+1} = -1$.

$$(4k^2q^2 + 8kq + 4) * a(km+1) \equiv (2kq+1)^{(2kq+2)} - 1 \pmod{8q}$$

$$(4k^2q^2 + 4)* a(km+1) \equiv ((2kq+1)^2)^{(kq+1)} - 1 \pmod{8q}$$

$$(4k^2q^2 + 4)* a(km+1) \equiv (4k^2q^2 + 4kq + 1)^{(kq+1)} - 1 \pmod{8q}$$

Now, if k is even then 4kq ≡ 0 (mod 8q) so we have:

$$4 * a(km+1) \equiv (1)^{(kq+1)} - 1 = 0 \pmod{8q}$$

This tells us that if k and m are both even, 4*a(km+1) is a multiple of 4m, so a(km+1) is a multiple of m. That is:

a(km+1) ≡ 0 ≡ ceiling(km/2) (mod m) for even k and even m.

It remains to prove a(km+1) ≡ ceiling(km/2) (mod m) for odd k and even m.

Now suppose k is odd, say k=2r+1 and m is even, m=2q.

Earlier (in the proof of Theorem III) I proved a binomial identity:

$$\frac{n+1}{2}=\sum_{k=2}^{n+1}(-1)^{n+1-k}\cdot\binom{n+1}{k}\cdot 2^{k-2}$$ for odd n, n > 0, and **[†]**

$$-\frac{n}{2}=\sum_{k=2}^{n+1}(-1)^{n+1-k}\cdot\binom{n+1}{k}\cdot 2^{k-2}$$ for even n, n > 0

We also have this formula for a(n):

$$a(n)=(-1)^n+\sum_{k=2}^{n+1}(-1)^{n+1-k}\cdot\binom{n+1}{k}\cdot(n+1)^{k-2}$$ for n > 0

$$a(km+1)=(-1)^{km+1}+\sum_{i=2}^{km+2}(-1)^{km+2-i}\cdot\binom{km+2}{i}\cdot(km+2)^{i-2}$$ for n = km+1

Now turn that into a congruence mod m. Also note that since m is even, km+1 is odd, so $(-1)^{km+1} = -1$. In the congruence, we can replace $(km+2)^{i-2}$ by 2^{i-2}.

$$a(km+1)\equiv -1+\sum_{i=2}^{km+2}(-1)^{km+2-i}\cdot\binom{km+2}{i}\cdot 2^{i-2}$$ (mod m)

Now the summation here is equal to (km+2)/2, by one of the binomial identities stated a few paragraphs ago; substitute **[†]** with n = km+1:

$$a(km+1)\equiv -1+\frac{km+2}{2}$$ (mod m) for odd k and even m

Since m is even, ½m is an integer, and we have:

a(km+1) ≡ –1 + ½km + 1 (mod m)
a(km+1) ≡ ½km = ceiling(km/2) (mod m) for odd k and even m

It still remains to show, for positive integers m and k:

For odd m, a(km-1) ≡ (-1)^(k+1) (mod m)
For even m, a(km-1) ≡ (km/2) – 1 (mod m)

Now take n=km–1. The sequence a(n) is defined for n ≥ 0 so here we stipulate k > 0. We want to prove that, mod m, a(km-1) is congruent to (-1)^(k+1) for odd m, and (km/2)–1 for even m. If m=1 the congruence is satisfied trivially so now we will assume m > 1 so km-1 > 0, and we use this formula I derived earlier:

$$a(n)=(-1)^n+\sum_{i=0}^{n-1}(-1)^{n+1-i}\cdot\binom{n+1}{i+2}\cdot(n+1)^i \quad \text{for } n > 0$$

$$a(km-1)=(-1)^{km-1}+\sum_{i=0}^{km-2}(-1)^{km-i}\cdot\binom{km}{i+2}\cdot(km)^i$$

We are evaluating the congruence mod m, so all the terms in the summation are zero other than for i=0. So we are left with:

a(km–1) ≡ $(–1)^{km–1}$ + $(–1)^{km}$ * C(km, 2) (mod m) **[‡]**

First suppose m is even; then ½m is an integer, and we have:

a(km–1) ≡ –1 + C(km, 2) (mod m)
a(km–1) ≡ –1 + ½(km)(km–1) (mod m)
a(km–1) ≡ –1 + k(½m)(km–1) (mod m)
a(km–1) ≡ –1 + k(½m)(0–1) (mod m)
a(km–1) ≡ –1 – ½km (mod m)

And since the congruence is mod m, we can add km to the right-hand side, to get

a(km–1) ≡ ½km – 1 (mod m) for even m.

Now suppose m is odd and consider **[‡]**. We want to compute C(km, 2) mod m. Consider the parity of k. If k is even, then ½km is an integer congruent to 0 mod m. If k is odd, then ½(km–1) is an integer, and km is congruent to 0 mod m. Either way, we have ½km(km–1) = C(km, 2) ≡ 0 (mod m).

Substitute in **[‡]**:

a(km–1) ≡ $(–1)^{km–1}$ + $(–1)^{km}$ * C(km, 2) (mod m)
a(km–1) ≡ $(–1)^{km–1}$ + 0 = $(–1)^{km–1}$ (mod m) for odd m.

And for odd m, km–1 has opposite parity to k. Therefore,

$a(km-1) \equiv (-1)^{k+1} \pmod{m}$ for odd m

Now I have proved, for positive integers k and m:

```
             a(km)   ≡ (–1)^(km)      (mod m)
             a(km+1) ≡ ceiling(km/2) (mod m)
For odd m,  a(km-1) ≡ (–1)^(k+1)     (mod m)
For even m, a(km-1) ≡ (km/2) – 1     (mod m)
```

We can recast these congruences, eliminating k from the right side, by considering even k and odd k separately.

First suppose k is even. Then km is even, and ½k is an integer, so:

```
a(km)   ≡ (–1)^(km)             = 1  (mod m)
a(km+1) ≡ ceiling(km/2) = (½k)m ≡ 0  (mod m)
For odd m,  a(km–1) ≡ (–1)^(k+1) = –1  (mod m)
For even m, a(km–1) ≡ (km/2) – 1 = (½k)m – 1 ≡ –1  (mod m)
```

Now suppose k is odd. It follows that ½(k-1) is an integer, and also that km has the same parity as m. This is going to be just a little trickier than the case for k even.

a(km) ≡ (–1)^(km) ≡ (–1)^m (mod m).

a(km+1) ≡ ceiling(km/2) (mod m)
subtract ½m(k-1) from the right-hand side, which is an integer divisible by m since k is odd:
a(km+1) ≡ ceiling(km/2) – ½m(k-1) (mod m)
then if m is even, the right-hand side is:
½km – ½(km – m) = ½m,
and if m is odd the right-hand side is :
½(km+1) – ½(km – m) = ½(m+1)
so for all m we have, when k is odd:
a(km+1) ≡ ceiling(m/2) (mod m)

Now consider a(km–1) (mod m) for k odd. We have already proved:

```
For odd m,  a(km-1) ≡ (–1)^(k+1)     (mod m)
For even m, a(km-1) ≡ (km/2) – 1     (mod m)
```

When k and m are both odd, we have:

$$a(km-1) \equiv (-1)^{(k+1)} = 1 \pmod{m}$$

And when k is odd and m is even, we have:

$$a(km-1) \equiv (km/2) - 1 \pmod{m}$$
$$a(km-1) \equiv k(\tfrac{1}{2}m) - 1 + m*\tfrac{1}{2}(k+1) \pmod{m}$$
$$a(km-1) \equiv -1 + \tfrac{1}{2}m = m/2 - 1 \pmod{m}$$

So that completes the proof of this theorem. We have shown that for positive integers k and m,

For even k:

$a(km) \equiv 1 \pmod{m}$
$a(km+1) \equiv 0 \pmod{m}$
$a(km-1) \equiv -1 \pmod{m}$

For odd k:

$a(km) \equiv (-1)^m \pmod{m}$
$a(km+1) \equiv \text{ceiling}(m/2) \pmod{m}$
$a(km-1) \equiv 1 \pmod{m}$ for m odd
$a(km-1) \equiv m/2 - 1 \pmod{m}$ for m even

Corollaries:

For any even n, $n/2$ divides $a(n) + a(n-1)$.
(Take $m = n/2$ and $k = 2$.)

For any odd n, n divides $a(n) + a(n-1)$.
(Take $m = n$ and $k = 1$.)

The sum of two adjacent terms of the sequence, $a(n) + a(n-1)$, is never prime; it has as a factor $n/2$ (if n is even) or n (if n is odd). (Including the special cases, $a(1)+a(0) = 1$ and $a(2)+a(1)=1$.) Moreover, for positive integers k and m:

$a(km) + a(km-1) \bmod m = 0$ for k even;
$a(km) + a(km-1) \bmod m = 0$ for k and m both odd; and
$a(km) + a(km-1) \bmod m = m/2$ for k odd and m even.

For any nonnegative integers k and m, $a(2km+1)$ and $a(2km)-1$ are both multiples of m.

Also, by setting k=1 it follows that a(n) ≡ (-1)^n (mod n), so n divides a(n)+1 for n odd, a(n)-1 for n even.

One other thing: note the overlap between A081215 and A193746

```
A081215(3) =        5 = A193746(4)
A081215(5) =      434 = A193746(6)
A081215(7) =    90075 = A193746(8)
A081215(9) = 34867844 = A193746(10)
A081215(13) = A193746(14)
A081215(15) = A193726(16)
A081215(17) = A193726(18)
```

but A081215(11) ≠ A193746(12)

By definition, A193746(n) satisfies:

n^2 * A193746(n) + 1 = j^n for some integer j.

Now if n is even, then
n^2 * A081215(n-1) + 1 = $(n-1)^n$

But A193746(n) is defined as the *smallest* k such that k*n^2 + 1 is an nth power. Can we state a rule descibing for which n, A193746(n) = A081215(n-1)? I don’t know.

XIII. For n > 2, a(n) mod (n^2 + 1) = r(n), where
r(n) is defined as follows for h = 0, 1, 2, ...:

```
r(4h)   = 8*h^2 –  2*h + 1
r(4h+1) = 8*h^2 +  8*h + 2
r(4h+2) = 8*h^2 +  6*h + 1
r(4h+3) = 8*h^2 + 12*h + 5
```

Proof: First we show that for n > 2, r(n) so defined satisfies 0 ≤ r(n) < (n^2 + 1). That’s the easy part.

We don’t have to worry about n = 0, 1, or 2. Now suppose n = 3. We have r(n) = r(0*h + 3) = 8*0 + 12*0 + 5 = 5. Thus 0 ≤ r(3) < (3^2 + 1) = 10. So now we just need to think about n ≥ 4, i.e. h ≥ 1. We need to show that 0 ≤ r(n) < n^2 + 1. From the definitions of r(4h+1) through r(4h+3) it is clear that those r(n) will be positive for all h ≥ 1, since they are each the sum of three positive numbers. For r(4h) it should also be clear that r(4h) is positive because 8h^2 > 2h for all h ≥ 1. Now to show that r(n) < n^2+1, start with h = 1. We can verify that:

```
r(4) =  7 < 17
r(5) = 18 < 26
r(6) = 15 < 37
r(7) = 25 < 50
```

Now suppose h ≥ 2 and consider each of r(4h) through r(4h+3) subtracted from 16h^2 = n^2:

```
16h^2 – r(4h)   = 8h^2 + 2h – 1
16h^2 – r(4h+1) = 8h^2 – 8h – 2
16h^2 – r(4h+2) = 8h^2 – 6h – 1
16h^2 – r(4h+3) = 8h^2 – 12h – 5
```

The polynomials on the right-hand side of these equations are all positive for h = 2 and they are strictly increasing for h ≥ 2 because the value of the first derivative is positive. Therefore 0 ≤ r(n) < n^2+1 for n > 2.

This means we just need to show a(n) ≡ r(n) (mod n^2 + 1) for n > 2 and we will have shown a(n) mod (n^2 + 1) = r(n).

Notice that (n+1)^2 ≡ 2n (mod n^2 + 1).

Because (n+1)^2 * a(n) = n^(n+1) + (−1)^n, we get:

2n * a(n) ≡ n^(n+1) + (−1)^n (mod n^2 + 1)

First suppose n is even, say n = 2j. Then:

4j * a(n) ≡   n * (n^2)^j + 1 (mod n^2 + 1)
4j * a(n) ≡ 2j * (−1)^j + 1 (mod n^2 + 1)

Now multiply through by j:
4j^2 * a(n) ≡ 2j^2 * (−1)^j + j (mod n^2 + 1)
And then since 4j^2 = n^2 ≡ −1 (mod n^2 + 1), we have:
−a(n) ≡ 2j^2 * (−1)^j + j (mod n^2 + 1)
 a(n) ≡ 2j^2 * (−1)^(j+1) − j (mod n^2 + 1)

Now first suppose j is even; say j = 2h and notice that n = 4h.

Now
 a(n) ≡ 8h^2 * (−1) − 2h (mod n^2 + 1)
and we can add n^2 + 1 = 16h^2 + 1 to the right-hand side:

 a(n) ≡ 16h^2 + 1 − 8h^2 − 2h (mod n^2 + 1)
 a(n) ≡ 8h^2 − 2h + 1 (mod n^2 + 1), where n = 4h

which is exactly what we needed to prove for the case n mod 4 = 0.

Still in the case where n is even, n = 2j, now suppose j is odd; say j = 2h + 1 so n = 4h + 2.

We previously had:
 a(n) ≡ 2j^2 * (−1)^(j+1) − j   (mod n^2 + 1)
 a(n) ≡ 2*(2h + 1)^2 − (2h + 1) (mod n^2 + 1)
 a(n) ≡ (8h^2 + 8h + 2) − (2h + 1) (mod n^2 + 1)
 a(n) ≡ 8h^2 + 6h + 1   (mod n^2 + 1), where n = 4h+2

which is exactly what we needed to prove for the case n mod 2 = 2.

So we have proved the theorem for n even.

Now suppose n is odd, n > 2. Say n = 2j + 1.

We need to pause to ask, if n is odd, what is the parity of a(n)? The answer is, it depends whether n mod 4 is 1 or 3.

We have a(n) = (n^(n+1) + (-1)^n) / (n+1)^2

Now if n mod 4 is 1, then the denominator, (n+1)^2, is divisible by 4 but not 8. Whereas the numerator, n^(n+1) + (-1)^n *is* divisible by 8. Why? Because mod 8, n must be either 1 or 5. If n is 1 mod 8, then the numerator is 1-1=0 mod 8. And if n is 5 mod 8, it also turns out that the numerator is 1-1=0 mod 8, because 5 raised to an even power is always 1, mod 8. Therefore, if n mod 4 = 1, then a(n) is even.

Now suppose n mod 4 = 3 and examine this formula for a(n):

(iii) $a(n)=(-1)^n+\sum_{k=0}^{n-3}(-1)^{(n+1-k)}*\binom{n+1}{k+2}*(n+1)^k$ for n > 2

Notice that (n+1) is even, so all values in the summation for k > 0 are even. Disregarding those, we have the following:

a(n) ≡ (-1)^n + (-1)^(n+1)*C(n+1, 2)
     = –1 + n(n+1)/2

Since n mod 4 = 3, n(n+1) is divisible by 4, so n(n+1)/2 is even, and thus a(n) is odd.

We’ve now shown that if n mod 4 is 1, then a(n) is even, while if n mod 4 is 3, then a(n) is odd.

Now we are going to consider congruences mod 2j^2 + 2j + 1. That formula is equal to (n^2 + 1)/2. In the end it will be easy to convert. Since n is odd, (n^2 + 1)/2 is an integer.

Note that
 n^2 + 1 ≡ 0 (mod 2j^2 + 2j + 1)
∴ (n + 1)^2 ≡ 2n (mod 2j^2 + 2j + 1), and
  n^2 ≡ –1 (mod 2j^2 + 2j + 1), and also
2j^2 + 2j ≡ –1 (mod 2j^2 + 2j + 1)
  n^(2j+2) ≡ (–1)^(j+1) (mod 2j^2 + 2j + 1)

By the definition of a(n), and using the fact n is odd,

(n+1)^2 * a(n) = n^(n+1) + (–1)^n

$$2n * a(n) \equiv n^{(2j+2)} - 1 \qquad (\text{mod } 2j^2 + 2j + 1)$$
$$2n * a(n) \equiv (-1)^{(j+1)} - 1 \qquad (\text{mod } 2j^2 + 2j + 1)$$

First suppose j is even. Say j = 2h so n = 4h + 1. Then:

$$2n * a(n) \equiv -2 \qquad (\text{mod } 2j^2 + 2j + 1)$$

But the modulus is an odd number, so we can divide both sides of the congruence by 2:

$$n * a(n) \equiv -1 \equiv n^2 \qquad (\text{mod } 2j^2 + 2j + 1)$$

Now, since n=2j+1, n and j must be coprime, which means that n and (n + 2j^2) = (2j^2 + 2j + 1) are coprime, so we can divide through by n:

$$a(n) \equiv n \ (\text{mod } 2j^2 + 2j + 1)$$

To summarize, we have shown that if n is odd, n=2j+1, and j is even, j=2h, so that n=4h+1, then
a(n) ≡ n (mod 2j^2 + 2j + 1).

But earlier, we showed that if n=4h+1 then a(n) is even.

Since a(n) is even and n is odd, their difference is odd, and in particular a(n) – n is an odd multiple of 2j^2 + 2j + 1. We can say:

$$(2z+1)*(2j^2 + 2j + 1) = a(n) - n \text{ for some integer } z.$$

$$2z*(2j^2 + 2j + 1) + (2j^2 + 2j + 1) = a(n) - n$$

But 2(2j^2 + 2j + 1) = n^2 + 1 since n = 2j+1. So,

$$z * (n^2 + 1) = (a(n) - n) - (2j^2 + 2j + 1)$$

Therefore:

$$a(n) \equiv n + 2j^2 + 2j + 1 \ (\text{mod } n^2 + 1)$$

Now remember we have n mod 4 = 1 and n=2j+1 and j=2h.

$$a(n) \equiv n + 2j^2 + 2j + 1 \ (\text{mod } n^2 + 1)$$

$$a(n) \equiv (4h + 1) + 8h^2 + 4h + 1 \pmod{n^2 + 1}$$
$$a(n) \equiv 8h^2 + 8h + 2 \pmod{n^2 + 1}$$

So now we’ve proved the theorem for $n \bmod 4 = 1$. All that’s left is the case $n \bmod 4 = 3$.

So, earlier we showed that for n odd, $n=2j+1$,
$$2n * a(n) \equiv (-1)^{(j+1)} - 1 \qquad \pmod{2j^2 + 2j + 1}$$

Now suppose j is odd, $j=2h+1$, so $n=4h+3$. $(-1)^{(j+1)} = 1$ and thus:

$$2n * a(n) \equiv 0 \qquad \pmod{2j^2 + 2j + 1}$$

But the modulus is odd, so as before we can divide through by 2:

$$n * a(n) \equiv 0 \qquad \pmod{2j^2 + 2j + 1}$$

And we can multiply through by n:

$$n^2 * a(n) \equiv 0 \qquad \pmod{2j^2 + 2j + 1}$$

But then since $n^2 = 4j^2 + 4j + 1 = 2*(2j^2 + 2j + 1) - 1$,

$$(-1) * a(n) \equiv 0 \qquad \pmod{2j^2 + 2j + 1}$$

$$a(n) \equiv 0 \pmod{2j^2 + 2j + 1}$$

But earlier, we showed that if $n=4h+3$ then $a(n)$ is odd.

Since $a(n)$ is odd, it is an odd multiple of $2j^2 + 2j + 1$. We can say, for some integer z:

$$\begin{aligned} a(n) &= (2z+1) * (2j^2 + 2j + 1) \\ &= 2z*(2j^2 + 2j + 1) + (2j^2 + 2j + 1) \\ &= z * (n^2 + 1) \qquad + (2j^2 + 2j + 1) \end{aligned}$$

Therefore
$$\begin{aligned} a(n) &\equiv 2j^2 + 2j + 1 \pmod{n^2 + 1} \\ &= 2*(2h+1)^2 + 2(2h+1) + 1 \\ &= 8h^2 + 8h + 2 + 4h + 2 + 1 \\ &= 8h^2 + 12h + 5 \end{aligned}$$

So now we’ve proved the theorem for n mod 4 = 3. And that concludes the proof of the whole theorem:

For n > 2, a(n) mod (n^2 + 1) = r(n), where
r(n) is defined as follows for h = 0, 1, 2, ...:
r(4h)   = 8*h^2 – 2*h + 1   = A185438(h)
r(4h+1) = 8*h^2 + 8*h + 2   = 1 + A069129(h)
r(4h+2) = 8*h^2 + 6*h + 1   = A014634(h)
r(4h+3) = 8*h^2 + 12*h + 5   = A060820(h+1)

Q.E.D.

We can also write r(n) as follows:
For n mod 4 = 0, r(n) = ½(n^2 – n + 2) = A152947(n+1)
= A000124(n-1) for n>0
For n mod 4 = 1, r(n) = ½(n^2 + 2n + 1) = ½(n+1)^2
For n mod 4 = 2, r(n) = ½(n^2 – n   ) = A161680(n)
For n mod 4 = 3, r(n) = ½(n^2   + 1) = ½(A002522(n))

We can also show that for n>3,
r(n) = r(n-1) – r(n-2) + r(n-3) – (n mod 4) +
(4*n – 5)*(n mod 2) + 1

Start with n mod 4 = 0. For convenience say n = 4h + 4. Now we need to show:
8*(h+1)^2 – 2*(h+1) +1 = r(4h+3) – r(4h+2) + r(4h+1)
– (n mod 4) + (4*n – 5)*(n mod 2) + 1

r(4h+3) – r(4h+2) + r(4h+1)
– (n mod 4) + (4*n – 5)*(n mod 2) + 1

= (8*h^2 + 12*h + 5) – (8*h^2 + 6*h + 1) +
(8*h^2 + 8*h + 2) – 0 + (4*n – 5)*0 + 1

= 8h^2 + 14h + 7

That was the right-hand side of the equation to prove. Now the left-hand side:

8*(h+1)^2 – 2*(h+1) +1
=8h^2 +16h + 8 – 2h – 2 + 1
=8h^2 +14h + 7

Now suppose n mod 4 = 1 and say n=4h+5. We need to show:

```
8*(h+1)^2 + 8*(h+1) + 2 = r(4h+4) – r(4h+3) + r(4h+2)
– (n mod 4) + (4*n – 5)*(n mod 2) + 1

r(4h+4) – r(4h+3) + r(4h+2)
– (n mod 4) + (4*n – 5)*(n mod 2) + 1

= ( 8h^2 +14h + 7) – ( 8*h^2 + 12*h + 5) + ( 8*h^2 +  6*h + 1)
   – 1 + (4*(4h+5) – 5) + 1

= 8h^2 + 24h + 18
```

Now the left-hand side:

```
8*(h+1)^2 + 8*(h+1) + 2
=8h^2 + 24h + 18
```

Now suppose n mod 4 = 2 and say n=4h+6. Now we need to show:

```
8*(h+1)^2 +  6*(h+1) + 1 = r(4h+5) – r(4h+4) + r(4h+3)
                     – (n mod 4) + (4*n – 5)*(n mod 2) + 1

r(4h+5) – r(4h+4) + r(4h+3)
– (n mod 4) + (4*n – 5)*(n mod 2) + 1

=  (8h^2 + 24h + 18) – (8h^2 +14h + 7) + ( 8*h^2 + 12*h + 5)
    – 2 + (4*(4h+2) – 5)*0 + 1

=  8h^2 + 22h + 15
```

Now the left-hand side of the equation we need to prove:

```
8*(h+1)^2 +  6*(h+1) + 1
= 8h^2 + 22h + 15
```

Finally, suppose n mod 4 is 3 and let n=4h+3. We need to show:

```
8*h^2 + 12*h + 5 = r(4h+2) – r(4h+1) + r(4h)
                    – (n mod 4) + (4*n – 5)*(n mod 2) + 1

r(4h+2) – r(4h+1) + r(4h)
 – (n mod 4) + (4*n – 5)*(n mod 2) + 1

=  (8*h^2 + 6*h + 1) – (8*h^2 +  8*h + 2) + (8*h^2 – 2*h + 1)
     – 3 + (4*(4h+3) – 5)*1 + 1
```

```
= 8h^2 + 12h + 5
Q.E.D.

Another recurrence relation, apparently, is the following:

r(n) = r(n–4) + (4n–10) + 2*(n mod 2)*(n+2 mod 4)
r(n) = r(n+4) – (4n– 6) – 2*(n mod 2)*(n+2 mod 4)

[these seem true, but not sure how to prove them]
```

XIV. [Conjecture]:

For n > 2, a(n) mod (n^3 – 1) = r(n), where r(n) is defined as follows for h = 0, 1, 2, ...:

```
r(6h)   = 108*h^3 + 18*h^2  -   3*h
r(6h+1) = 108*h^3 + 18*h^2  +   3*h
r(6h+2) = 108*h^3 + 162*h^2 +  69*h + 8
r(6h+3) = 108*h^3 + 126*h^2 +  45*h + 5
r(6h+4) = 108*h^3 + 234*h^2 + 171*h + 41
r(6h+5) = 108*h^3 + 270*h^2 + 225*h + 62
```

We can also write r(n) as follows:

For n mod 6 = 0, $r(n) = \frac{1}{2}(n^3 + n^2 - n)$

For n mod 6 = 1, $r(n) = \frac{1}{2}(n^3 - 2n^2 + 2n - 1)$

For n mod 6 = 2, $r(n) = \frac{1}{2}(n^3 + 3n^2 - n - 2)$

For n mod 6 = 3, $r(n) = \frac{1}{2}(n^3 - 2n^2 + 1)$

For n mod 6 = 4, $r(n) = \frac{1}{2}(n^3 + n^2 + n - 2)$

For n mod 6 = 5, $r(n) = \frac{1}{2}(n^3 - 1)$

[conjectured]

XV. [Conjecture]:

For n > 4, a(n) mod (n^4 + 1) = r(n), where
r(n) is defined as follows for h = 0, 1, 2, ...:

```
r(8h)   = 2048*h^4 –  256*h^3 +  32*h^2  –  4*h + 1
r(8h+1) = 2048*h^4 + 1536*h^3 + 320*h^2  + 32*h + 2
r(8h+2) = 2048*h^4 + 1280*h^3 + 288*h^2  + 28*h + 1
r(8h+3) = 2048*h^4 + 4096*h^3 + 2816*h^2 + 816*h + 87
r(8h+4) = 2048*h^4 + 3328*h^3 + 1952*h^2 + 484*h + 41
r(8h+5) = 2048*h^4 + 5632*h^3 + 5760*h^2 + 2592*h + 434
r(8h+6) = 2048*h^4 + 5888*h^3 + 6304*h^2 + 2980*h + 525
r(8h+7) = 2048*h^4 + 7168*h^3 + 9408*h^2 + 5488*h + 1201
```

Another way of defining r(n) is:

if n mod 8 is 0, r(n) = $\frac{1}{2}(n^4 - n^3 + n^2 - n + 2)$
= 1 + A071252(n)
= $\frac{1}{2}$(1 + A060884(n))

if n mod 8 is 1, r(n) = $\frac{1}{2}(n^4 + 2n^3 - 2n^2 + 2n + 1)$

if n mod 8 is 2, r(n) = $\frac{1}{2}(n^4 - 3n^3 + 3n^2 - n)$
= A019582(n)
= $\frac{1}{2}$(A179824(n)) for n ≥ 2

if n mod 8 is 3, r(n) = $\frac{1}{2}(n^4 + 4n^3 - 2n^2 + 3)$

if n mod 8 is 4, r(n) = $\frac{1}{2}(n^4 - 3n^3 + n^2 + n - 2)$

if n mod 8 is 5, r(n) = $\frac{1}{2}(n^4 + 2n^3 - 2n + 3)$

if n mod 8 is 6, r(n) = $\frac{1}{2}(n^4 - n^3 - n^2 + n)$
= $\frac{1}{2}$(A047927(n+1)) for n ≥ 1
= 3(A002417(n-1)) for n ≥ 2

if n mod 8 is 7, r(n) = $\frac{1}{2}(n^4 + 1)$
= $\frac{1}{2}$(A002523(n))
= A175110((n–1)/2) for odd n

[Conjectured.]
Verified for n up to 51000, i.e. h up to 6375.

XVI. [Conjecture]:

For n > 5, a(n) mod (n^5 – 1) = r(n), where
r(n) is defined as follows for h = 0, 1, 2, ...:

```
r(10h)   = 50000*h^5 +   5000*h^4 –    500*h^3 +     50*h^2 –      5*h
r(10h+1) = 50000*h^5 +  15000*h^4 +   2000*h^3 +    100*h^2 +      5*h
r(10h+2) = 50000*h^5 +  65000*h^4 +  30500*h^3 +   6850*h^2 +    755*h +    32
r(10h+3) = 50000*h^5 +  55000*h^4 +  23000*h^3 +   4400*h^2 +    345*h +     5
r(10h+4) = 50000*h^5 + 125000*h^4 + 118500*h^3 +  54250*h^2 +  12125*h +  1064
r(10h+5) = 50000*h^5 + 105000*h^4 +  86000*h^3 +  34000*h^2 +   6365*h +   434
r(10h+6) = 50000*h^5 + 165000*h^4 + 215500*h^3 + 139450*h^2 +  44775*h +  5713
r(10h+7) = 50000*h^5 + 165000*h^4 + 217000*h^3 + 142200*h^2 +  46435*h +  6045
r(10h+8) = 50000*h^5 + 205000*h^4 + 336500*h^3 + 276350*h^2 + 113525*h + 18659
r(10h+9) = 50000*h^5 + 225000*h^4 + 405000*h^3 + 364500*h^2 + 164025*h + 29524
```

Another way of defining r(n) is:

if n mod 10 is 0, $r(n) = \frac{1}{2}(n^5 + n^4 - n^3 + n^2 - n)$
if n mod 10 is 1, $r(n) = \frac{1}{2}(n^5 - 2n^4 + 2n^3 - 2n^2 + 2n - 1)$
if n mod 10 is 2, $r(n) = \frac{1}{2}(n^5 + 3n^4 - 3n^3 + 3n^2 - n - 2)$
if n mod 10 is 3, $r(n) = \frac{1}{2}(n^5 - 4n^4 + 4n^3 - 2n^2 + 1)$
if n mod 10 is 4, $r(n) = \frac{1}{2}(n^5 + 5n^4 - 3n^3 + n^2 + n - 4)$
if n mod 10 is 5, $r(n) = \frac{1}{2}(n^5 - 4n^4 + 2n^3 - 2n + 3)$
if n mod 10 is 6, $r(n) = \frac{1}{2}(n^5 + 3n^4 - n^3 - n^2 + 3n - 4)$
if n mod 10 is 7, $r(n) = \frac{1}{2}(n^5 - 2n^4 + 2n^2 - 2n + 1)$
if n mod 10 is 8, $r(n) = \frac{1}{2}(n^5 + n^4 + n^3 - n^2 + n - 2)$
if n mod 10 is 9, $r(n) = \frac{1}{2}(n^5 - 1)$

[Conjectured.]

XVII. Conjecture: Suppose k is any positive integer, and n an integer with n > k. Then a(n) mod ($n^k + (-1)^k$) can be expressed by a set of 2k polynomials in n of degree k, a different polynomial depending on n mod 2k.

If n mod 2k = 0, then a(n) mod (n^k + (–1)^k) =
$\frac{1}{2}(n^k - n^{k-1} + n^{k-2} - \ldots + (-1)^k * 2)$

If n ≡ –1 (mod 2k), then a(n) mod (n^k + (–1)^k) =
½(n^k + (-1)^k)

This is a generalization of:

Theorem III. For n > 2, a(n) mod (n – 1) = floor(n/2).
Theorem XIII. For n > 2, a(n) mod (n^2 + 1) = ...
Conjecture XIV. For n > 2, a(n) mod (n^3 – 1) = ...
Conjecture XV. For n > 4, a(n) mod (n^4 – 1) = ...
Conjecture XVI. For n > 5, a(n) mod (n^5 – 1) = ...

XVIII. [Conjecture]:

For n odd, $n>2$, $a(n) \bmod (n-1)^2/2 = (n-1)/2$

i.e. for $m > 0$, $a(2m+1) \bmod 2m^2 = m$

For example, $a(11) \bmod 50 = 21794641505 \bmod 50 = 5$

$a(13) \bmod 72 = 20088655029078 \bmod 72 = 6$

Verified for m = 1 ... 5000.

XIX. [Conjecture]: For any nonnegative integer n,
$2*a(n) \equiv n^n - n*(-1)^n \pmod{n^2 + 1}$.

Notice that the formula on the right-hand side of that congruence is A066068 for n odd, and A061190 for n even.

Verified for n = 0 ... 1000.

XX. [Conjecture]: For any integer $m \geq 2$,
$a(2m+1) \bmod m^3 = m$.

```
  For example: a(11) mod 125 =    21794641505 mod 125 = 5
               a(13) mod 216 = 20088655029078 mod 216 = 6
```

Verified for n = 2 ... 1000.

XXI. [Conjecture]: For a prime p other than 2 or 3, $a((p-3)/2) \equiv 0, 8, \text{ or } -8 \pmod{p}$.

In other words, the claim is that if 2n+3 is prime, then generally $a(n) \bmod (2n+3) \in \{0, 8, 2n-5\}$ (aside from n=2).

See OEIS A067076, “Numbers k such that 2*k + 3 is a prime.”

For example, $a(1) = 0 \equiv 0 \pmod{5}$
$a(2) = 1 \equiv 8 \pmod{7}$
$a(4) = 41 \equiv 8 \pmod{11}$
$a(5) = 434 \equiv -8 \pmod{13}$

$a(73) \equiv 0 \pmod{149}$
$a(74) \equiv 8 \pmod{151}$
$a(77) \equiv -8 \pmod{157}$
$a(80) \equiv 0 \pmod{163}$
$a(82) \equiv 0 \pmod{167}$

but $a(75) \equiv 14 \pmod{153}$; $a(76) \equiv 13 \pmod{155}$; $a(78) \equiv -2 \pmod{159}$; $a(79) \equiv -2 \pmod{161}$; $a(81) \equiv 5 \pmod{165}$, and 153, 155, 159, 161, and 165 are all composite.

There do exist some n not in A067076 for which $a(n) \bmod (2n+3) \in \{0, 8, 2n-5\}$. For example $a(31) \equiv 0 \pmod{65}$ and $a(58) \equiv -8 \pmod{119}$.

This conjecture has been verified for n = 1 ... 5000 (i.e. for all primes from 5 to 9973).

XXII. Miscellaneous Conjectures.

The following conjectures were discussed above, in the context of Theorem VI. They are repeated here for convenience.

```
a(n) - a(n+8)     ==   4n (mod 24)  for n >= 0
a(n+2) – a(n+18)  ==   8n (mod 48)  for n >= 1
a(n+6) - a(n+38)  ==  16n (mod 96)  for n >= -3
a(n+8) - a(n+72)  ==  32n (mod 192) for n >= -5
a(n) - a(n+128)   ==  64n (mod 384) for n >= 3
a(n+8) - a(n+264) == 128n (mod 768) for n >= -1
```

Here are some other conjectures, all verified for values of n up to 5000:

```
a(4n) + a(4n+2) == 58 (mod 64) for n >= 1
a(4n+1) + a(4n+3) == 5 (mod 8) for n >= 0
a(4n+2) + a(4n+4) == 2 (mod 32) for n >= 1
a(4n+3) + a(4n+5) == 7 (mod 8) for n >= 0

a(10n) == 1 (mod 40)
a(10n+4) == 1 (mod 40)
a(10n+6) == 33 (mod 40)

a(30n) == 1 (mod 120)
a(30n+4) == 41 (mod 120)
a(30n+16) == 113 (mod 120)

a(60n+2) == 1 (mod 120)
a(60n+4) == 41 (mod 120)
a(60n+6) == 73 (mod 120)
a(60n+8) == 49 (mod 120)
```

The following conjectures were discussed above at Theorem IV:

a(2m+1) mod 4m = m for m>0.
[Verified up to m = 5000.]

```
Conjecture: for odd  m, a(2m-1) mod 4m =  m–1;
            for even m, a(2m-1) mod 4m = 3m–1  (m>0).
```
[Verified up to m = 5000.]

```
Conjecture: for m ≡ 1 (mod 3), a(2m) mod 3m = 1;
            for m ≡ 0 or 2 (mod 3), a(2m) mod 3m = 2m+1 (m>0).
```
[Verified up to m = 5000.]

Conjecture: for m mod 4 = 1, a(3m) mod 2m = 2m-1;
for m mod 4 = 3, a(3m) mod 2m = m-1;
for even m, a(3m) mod 2m = 1 (m>0).
[Verified up to m = 5000.]

Conjecture: for m mod 12 = 0, a(7m) mod 6m = 4m+1; (m>0)
for m mod 12 = 1, a(7m) mod 6m = 4m-1;
for m mod 12 = 2, a(7m) mod 6m = 1;
for m mod 12 = 3, a(7m) mod 6m = 5m-1;
for m mod 12 = 4, a(7m) mod 6m = 4m+1;
for m mod 12 = 5, a(7m) mod 6m = 6m–1;
for m mod 12 = 6, a(7m) mod 6m = 4m+1;
for m mod 12 = 7, a(7m) mod 6m = m-1;
for m mod 12 = 8, a(7m) mod 6m = 1;
for m mod 12 = 9, a(7m) mod 6m = 2m-1;
for m mod 12 =10, a(7m) mod 6m = 4m+1; and
for m mod 12 =11, a(7m) mod 6m = 3m-1.
[Verified up to m = 5000.]

Two conjectures concerning A081215(n) expressed in base (n–1) that were mentioned above after the proof of Theorem V:

For n odd, the last two digits of a(n) in base n-1 are 0 and (n-1)/2

For n even, the last two digits of a(n) in base n-1 are (n-2)/2 and n/2.

The following conjectures are mentioned above after Theorem XI:

a(3p+2) ≡ 7 (mod p) (for prime p > 3)
a(6p+2) ≡ 57 (mod p) (for prime p > 3)
a(8p-5) ≡ 39 (mod p) (seems to be true for all primes and many nonprimes, e.g. a(8*65-5) ≡ 39 (mod 65), a(8*66-5) ≡ 39 (mod 66).)
a(9p-7) ≡ (p-19)/2 (mod p) for odd prime p
a(9p+2) ≡ 455 (mod p) for any prime p

[End of document.]