Perfect Polynomials

modulo 2

Ugur Caner Cengiz

Lake Forest College

April 7, 2015

Outline

1. Definitions
   - modulo 2
   - What is "Perfect"?
   - Perfect Polynomials

Outline

1. Definitions
   - modulo 2
   - What is "Perfect"?
   - Perfect Polynomials
2. Previous Research
   - Others'
   - Ours

Outline

What do you mean by "modulo 2"?

- In simple terms, 'a mod b' gives the remainder when integer a is divided by non-zero integer b.

What do you mean by "modulo 2"?

- In simple terms, 'a mod b' gives the remainder when integer a is divided by non-zero integer b.

- Therefore, mod 2 is very simple: if the number is odd, then it is equivalent to 1 and if even, then it is equivalent to 0.

What do you mean by "modulo 2"?

- In simple terms, '*a* mod *b*' gives the remainder when integer *a* is divided by non-zero integer *b*.

- Therefore, mod 2 is very simple: if the number is odd, then it is equivalent to 1 and if even, then it is equivalent to 0.

- $13 \equiv 1$ and $54678 \equiv 0 \pmod 2$

Perfect Numbers

Sigma function σ

Definition

Lower case Greek letter sigma (σ) symbolizes an arithmetic function that sums the positive divisors of a positive integer.

$$\sigma(n) = \sum_{d|n} d$$

Definition

If $\sigma(n) = 2n$, then n is perfect.

Example

Perfect Numbers

Sigma function σ

Definition

Lower case Greek letter sigma (σ) symbolizes an arithmetic function that sums the positive divisors of a positive integer.

$$\sigma(n) = \sum_{d|n} d$$

Definition

If $\sigma(n) = 2n$, then n is perfect.

Example

- 6

Perfect Numbers

Sigma function σ

Definition

Lower case Greek letter sigma (σ) symbolizes an arithmetic function that sums the positive divisors of a positive integer.

$$\sigma(n) = \sum_{d|n} d$$

Definition

If $\sigma(n) = 2n$, then n is perfect.

Example

- 6
- $\sigma(6) = 1 + 2 + 3 + 6 = 12$

Perfect Numbers

Sigma function σ

Definition

Lower case Greek letter sigma (σ) symbolizes an arithmetic function that sums the positive divisors of a positive integer.

$$\sigma(n) = \sum_{d|n} d$$

Definition

If $\sigma(n) = 2n$, then n is perfect.

Example

- 6
- $\sigma(6) = 1 + 2 + 3 + 6 = 12$
- Hence, 6 is perfect.

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.
- $\sigma(2)=(2+1)$ and $\sigma(3)=(3+1)$

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.
- $\sigma(2)$=(2 + 1) and $\sigma(3)$=(3+1)
- $\sigma(2) \times \sigma(3)$=3 $\times$ 4 = 12 = $\sigma(6)$.

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.
- $\sigma(2)=(2+1)$ and $\sigma(3)=(3+1)$
- $\sigma(2) \times \sigma(3)=3 \times 4 = 12 = \sigma(6)$.
- $728 = 2^3 \times 7 \times 13$

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.
- $\sigma(2)=(2+1)$ and $\sigma(3)=(3+1)$
- $\sigma(2) \times \sigma(3)=3 \times 4 = 12 = \sigma(6)$.
- $728 = 2^3 \times 7 \times 13$
- $\sigma(728) = 1 + 2 + 4 + 7 + 8 + 13 + 14 + 26 + 28 + 52 + 56 + 91 + 104 + 182 + 364 + 728 = 1680$

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.
- $\sigma(2)=(2+1)$ and $\sigma(3)=(3+1)$
- $\sigma(2) \times \sigma(3) = 3 \times 4 = 12 = \sigma(6)$.
- $728 = 2^3 \times 7 \times 13$
- $\sigma(728) = 1 + 2 + 4 + 7 + 8 + 13 + 14 + 26 + 28 + 52 + 56 + 91 + 104 + 182 + 364 + 728 = 1680$
- Note that $\sigma(p^q) = (p^q + p^{q-1} + ... + p + 1)$

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.
- $\sigma(2)=(2 + 1)$ and $\sigma(3)=(3+1)$
- $\sigma(2) \times \sigma(3)=3 \times 4 = 12 = \sigma(6)$.
- $728 = 2^3 \times 7 \times 13$
- $\sigma(728) = 1 + 2 + 4 + 7 + 8 + 13 + 14 + 26 + 28 + 52 + 56 + 91 + 104 + 182 + 364 + 728 = 1680$
- Note that $\sigma(p^q) = (p^q + p^{q-1} + ... + p + 1)$
- So, $\sigma(2^3) \times \sigma(7) \times \sigma(13) = (8 + 4 + 2 + 1)(7 + 1)(13 + 1)$

Continuing on σ

Theorem

σ is multiplicative over integers.
If gcd(m,n) = 1, then $\sigma(mn) = \sigma(m) \times \sigma(n)$

Example

- $6 = 2 \times 3$ where 2 and 3 are prime.
- $\sigma(2)=(2+1)$ and $\sigma(3)=(3+1)$
- $\sigma(2) \times \sigma(3)=3 \times 4 = 12 = \sigma(6)$.
- $728 = 2^3 \times 7 \times 13$
- $\sigma(728) = 1 + 2 + 4 + 7 + 8 + 13 + 14 + 26 + 28 + 52 + 56 + 91 + 104 + 182 + 364 + 728 = 1680$
- Note that $\sigma(p^q) = (p^q + p^{q-1} + ... + p + 1)$
- So, $\sigma(2^3) \times \sigma(7) \times \sigma(13) = (8 + 4 + 2 + 1)(7 + 1)(13 + 1)$
- $\sigma(2^3) \times \sigma(7) \times \sigma(13) = 15 \times 8 \times 14 = 1680$

Polynomials mod 2

- For a polynomial mod 2, the coefficients are mod 2. Thus, $5x^7 + 9x^6 + 16x^5 + 48x^4 + x^3 + 4x^2 + 71x + 1 \equiv x^7 + x^6 + x^3 + x + 1$

Polynomials mod 2

- For a polynomial mod 2, the coefficients are mod 2. Thus, $5x^7+9x^6+16x^5+48x^4+x^3+4x^2+71x+1 \equiv x^7+x^6+x^3+x+1$
- $x^2+1=0$ has no real roots. It's irreducible.

Polynomials mod 2

- For a polynomial mod 2, the coefficients are mod 2. Thus, $5x^7 + 9x^6 + 16x^5 + 48x^4 + x^3 + 4x^2 + 71x + 1 \equiv x^7 + x^6 + x^3 + x + 1$
- $x^2 + 1 = 0$ has no real roots. It's irreducible.
- Consider $(x + 1)^2$ modulo 2

Polynomials mod 2

- For a polynomial mod 2, the coefficients are mod 2. Thus, $5x^7 + 9x^6 + 16x^5 + 48x^4 + x^3 + 4x^2 + 71x + 1 \equiv x^7 + x^6 + x^3 + x + 1$
- $x^2 + 1 = 0$ has no real roots. It's irreducible.
- Consider $(x + 1)^2$ modulo 2
- $(x + 1)^2 = (x + 1) \times (x + 1) = x^2 + 2x + 1^2$

Polynomials mod 2

- For a polynomial mod 2, the coefficients are mod 2. Thus, $5x^7 + 9x^6 + 16x^5 + 48x^4 + x^3 + 4x^2 + 71x + 1 \equiv x^7 + x^6 + x^3 + x + 1$
- $x^2 + 1 = 0$ has no real roots. It's irreducible.
- Consider $(x + 1)^2$ modulo 2
- $(x + 1)^2 = (x + 1) \times (x + 1) = x^2 + 2x + 1^2$
- $x^2 + 2x + 1^2 \equiv x^2 + 1 \pmod 2$

σ on polynomials

Definition

If $\sigma(A) = A$, then A is a perfect polynomial.

σ on polynomials

Definition

If σ(A) = A, then A is a perfect polynomial.

- For example, $x^2 + x = x \times (x + 1)$

σ on polynomials

Definition

If σ(A) = A, then A is a perfect polynomial.

- For example, $x^2 + x = x \times (x + 1)$
- $\sigma(x^2 + x) = (x^2 + x) + (x + 1) + x + 1 = x^2 + 3x + 2$

σ on polynomials

Definition

If σ(A) = A, then A is a perfect polynomial.

- For example, $x^2 + x = x \times (x + 1)$
- $\sigma(x^2 + x) = (x^2 + x) + (x + 1) + x + 1 = x^2 + 3x + 2$
- $x^2 + 3x + 2 \equiv x^2 + x \pmod 2$

σ on polynomials

Definition

If σ(A) = A, then A is a perfect polynomial.

- For example, $x^2 + x = x \times (x + 1)$
- $\sigma(x^2 + x) = (x^2 + x) + (x + 1) + x + 1 = x^2 + 3x + 2$
- $x^2 + 3x + 2 \equiv x^2 + x \pmod 2$
- So $\sigma(x^2 + x) = x^2 + x \pmod 2$
- $x^2 + x$ is a perfect polynomial mod 2.

Canaday, Gallardo and Rahavandrainy

- **E. F. Canaday**

- **Gallardo and Rahavandrainy**

Canaday, Gallardo and Rahavandrainy

- **E. F. Canaday**
- Perfect polynomials mod 2 exist in two ways: $x^h(x+1)^k A$ and B^2, where B is relatively prime to $x(x+1)$

- **Gallardo and Rahavandrainy**

Canaday, Gallardo and Rahavandrainy

- **E. F. Canaday**
- Perfect polynomials mod 2 exist in two ways:
  $x^h(x+1)^k A$ and B^2, where B is relatively prime to $x(x+1)$
- Also, he found an infinite class of perfects: $x^{2^n-1}(x+1)^{2^n-1}$

- **Gallardo and Rahavandrainy**

Canaday, Gallardo and Rahavandrainy

- **E. F. Canaday**
- Perfect polynomials mod 2 exist in two ways:
  $x^h(x+1)^kA$ and B^2, where B is relatively prime to $x(x+1)$
- Also, he found an infinite class of perfects: $x^{2^n-1}(x+1)^{2^n-1}$
- Conjecture that every perfect is divisible by $x(x+1)$
  In other words, no odd perfects
- **Gallardo and Rahavandrainy**

Canaday, Gallardo and Rahavandrainy

- **E. F. Canaday**
- Perfect polynomials mod 2 exist in two ways:
  $x^h(x+1)^k A$ and B^2, where B is relatively prime to $x(x+1)$
- Also, he found an infinite class of perfects: $x^{2^n-1}(x+1)^{2^n-1}$
- Conjecture that every perfect is divisible by $x(x+1)$
  In other words, no odd perfects

- **Gallardo and Rahavandrainy**
- Proved that odd perfects have at least 5 distinct irreducible factors.

Degree	Factorization into Irreducibles
5	$T(T+1)^2(T^2+T+1)$
	$T^2(T+1)(T^2+T+1)$
11	$T(T+1)^2(T^2+T+1)^2(T^4+T+1)$
	$T^2(T+1)(T^2+T+1)^2(T^4+T+1)$
	$T^3(T+1)^4(T^4+T^3+1)$
	$T^4(T+1)^3(T^4+T^3+T^2+T+1)$
15	$T^3(T+1)^6(T^3+T+1)(T^3+T^2+1)$
	$T^6(T+1)^3(T^3+T+1)(T^3+T^2+1)$
16	$T^4(T+1)^4(T^4+T^3+1)(T^4+T^3+T^2+T+1)$
20	$T^4(T+1)^6(T^3+T+1)(T^3+T^2+1)(T^4+T^3+T^2+T+1)$
	$T^6(T+1)^4(T^3+T+1)(T^3+T^2+1)(T^4+T^3+1)$

Figure: Canaday's list for perfects

The Algorithm to Find the Perfect Polynomials

- Check if $\sigma B = B$. Output B.

The Algorithm to Find the Perfect Polynomials

- Check if σB = B. Output B.
- If not, compute D where D = σ(B) / gcd(B, σ(B))

The Algorithm to Find the Perfect Polynomials

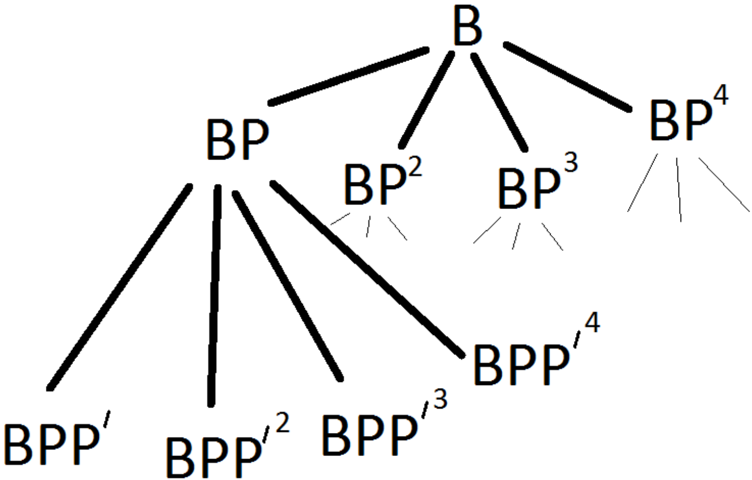
- Check if σB = B. Output B.
- If not, compute D where D = σ(B) / gcd(B, σ(B))
- If gcd(B, D) $>$ 1, then stop. No output!

The Algorithm to Find the Perfect Polynomials

- Check if σB = B. Output B.
- If not, compute D where D = σ(B) / gcd(B, σ(B))
- If gcd(B, D) $>$ 1, then stop. No output!
- If the polynomial passes the test on step 3, then let P be the greatest factor of D.

The Algorithm to Find the Perfect Polynomials

- Check if σB = B. Output B.
- If not, compute D where D = σ(B) / gcd(B, σ(B))
- If gcd(B, D) $>$ 1, then stop. No output!
- If the polynomial passes the test on step 3, then let P be the greatest factor of D.
- Restart the algorithm taking BP, BP^2, BP^3, ..., BP^k where degree of BP^k $< K$.


B
BP
BP2
BP3
BP4
BPP'
BPP'2
BPP'3
BPP'4

Beginning steps - primPerf()

```
def primPerf(B):
    if B == sumDivs4(B):
        return B
    else:
        D = (sumDivs4(B)/gcd(B, sumDivs4(B)))
        if gcd(D,B) != 1:
            return False
        else:
            F = D.factor()
            P = F[len(F)-1][0]
            check = False
            K = 1
            while (B*(P^K)).degree() <= 1000:
                check = primPerf(B*(P^K))
                if check == False:
                    K = K + 1
                else:
                    return primPerf((B*(P^K)))
                    break
```

Results up to degree 200

$x \times (x+1)^2 \times (x^2+x+1)$
$x \times (x+1)^2 \times (x^2+x+1)^2 \times (x^4+x+1)$
$(x+1) \times x^2 \times (x^2+x+1)$
$(x+1) \times x^2 \times (x^2+x+1)^2 \times (x^4+x+1)$
$x^3 \times (x+1)^4 \times (x^4+x^3+1)$
$x^3 \times (x+1)^6 \times (x^3+x+1) \times (x^3+x^2+1)$
$(x+1)^3 \times x^4 \times (x^4+x^3+x^2+x+1)$
$x^4 \times (x+1)^4 \times (x^4+x^3+1) \times (x^4+x^3+x^2+x+1)$
$x^4 \times (x+1)^6 \times (x^3+x+1) \times (x^3+x^2+1) \times (x^4+x^3+x^2+x+1)$
$(x+1)^3 \times x^6 \times (x^3+x+1) \times (x^3+x^2+1)$
$(x+1)^4 \times x^6 \times (x^3+x+1) \times (x^3+x^2+1) \times (x^4+x^3+1)$
$x \times (x+1)$
$x^3 \times (x+1)^3$
$x^7 \times (x+1)^7$
$x^{15} \times (x+1)^{15}$
$x^{31} \times (x+1)^{31}$ and $x^{63} \times (x+1)^{63}$

Speed

```
def sigma1(x, y):
  return (x^(y+1) - 1)/(x - 1)

def sigma2(x, y):
   sum = 0
   for pow in range(0, y+1):
     sum = sum + (x^pow)
  return sum
```

*sigma*1 and *sigma*2 speed testing

Dynamic Programming

```
import time
tic = time.clock()
sum = x^30
found = primPerf(sum)
if type(found)== type(x):
    print found, "=", found.factor()
toc = time.clock()
toc - tic

  0.000747000000182608

perfFinder(15)

  1 = 1
  degree =  0

  x^2 + x = x * (x + 1)
  degree =  2

  x^2 + x = x * (x + 1)
  degree =  2
```

Figure: FAST!

Summary

- A perfect polynomial equals the sum of its divisors.
- As Canaday thought there are no odd perfect polynomials up to degree 200.
- My program is relatively fast and finds the perfect polynomials.

- Future Plans
  - To check higher degrees
  - Show odd perfect polynomials mod 2 have at least 6 factors
  - Work on a paper

For Further Information

E.F. Canaday
The Sum of The Divisors of a Polynomial.
Duke Mathematical Journal, 8(4):721–737, 1941

L. Gallardo. and O. Rahavandrainy.
Odd Perfect Polynomials over F_2
Journal de Théeorie des Nombres de Bordeaux, 19(1):165–174, 2007.

L. Gallardo. and O. Rahavandrainy.
There is no odd perfect polynomial over F_2 with four prime factors
Portugaliae Mathematica, 66(2):131–145, 2009.

Thank You!

(Any Questions?)