The Basic Functions
Phi, Tau, Sigma
in Elementary Number Theory

Author: Jochen Ziegenbalg
Email: ziegenbalg.edu@gmail.com
Internet: https://jochen-ziegenbalg.github.io/root/

■ References

Mönkemeyer R.: Einführung in die Zahlentheorie; Verlage Schroedel und Schöningh, Hannover und Paderborn 1971
Ore O.: Number Theory and its History; Dover Publications Inc., New York 1948
Ore O.: Invitation to Number Theory; Mathematical Association of America, 1967 Yale University
Ziegenbalg J.: Elementare Zahlentheorie - Beispiele, Geschichte, Algorithmen; Harri Deutsch Verlag, Frankfurt am Main 2002

■ Basic concepts

Definition: An *arithmetic function* (in German: *zahlentheoretische Funktion*) is a function $f : \mathbb{N} \to \mathbb{R}$ or $f : \mathbb{N} \to \mathbb{C}$.

An arithmetic function f is called *multiplicative* if for all relatively prime (in German: *teilerfremd*) integers $m, n \in \mathbb{N}$ the following equation holds:

$$f(m \cdot n) = f(m) \cdot f(n).$$

Excercise: Show that for any multiplicative arithmetic function f the following equation holds: $f(1) = 1$.

Examples: Some typical arithmetical functions of number theory are (for $n \in \mathbb{N}$):

$$\begin{aligned}\tau(n) &= \text{the number of divisors of } n\\ \sigma(n) &= \text{the sum of divisors of } n\\ \varphi(n) &= \text{number of integers in } \{1,\ 2,\ 3,\ \ldots,\ n-1\} \text{ relatively prime to } n\\ &\ \text{(Euler } \varphi - \text{Function, Euler totient function)}\end{aligned}$$

Definition: Every integer n is a divisor of itself. It is called the improper divisor of n. All other divisors of n are called *proper divisors* (in German: *echte Teiler*), or in more archaic language, the *aliqout parts* (in Latin aliquot: dividing without remainder).

Sometimes it is more convenient to sum up the aliquot parts instead of all the divisors of n. For this purpose we define

$\sigma_0(n) =$ the sum of the proper divisors of n.

Obviously $\sigma_0(n) = \sigma(n) - n$.

Using these functions in *Mathematica*:

```
Divisors[24]

{1, 2, 3, 4, 6, 8, 12, 24}

AliquotParts[n_] := Drop[Divisors[n], -1]

AliquotParts[24]

{1, 2, 3, 4, 6, 8, 12}

Tau[n_] := Length[Divisors[n]];
Tau2[n_] :=
  Apply[Times, Map[Function[x, x + 1], Map[Last, FactorInteger[n]]]];
TauComp[n_] := {Timing[Tau[n]], Timing[Tau2[n]]}

Tau[24]

8

Tau2[24]

8

TauComp[2427382736428738372884342393 43]

{{0.06 Second, 24}, {0.07 Second, 24}}

Sigma[n_] := Apply[Plus, Divisors[n]];
Sigma0[n_] := Apply[Plus, AliquotParts[n]];

Sigma[24]

60

Sigma[28]

56
```

```
Sigma0[28]
```

```
28
```

```
EulerPhi[12]
```

```
4
```

```
EulerPhi[13]
```

```
12
```

```
EulerPhi[60]
```

```
16
```

```
EulerPhi[1]
```

```
1
```

The **Fundamental Theorem of Number Theory** (in German: Hauptsatz der Zahlentheorie / Fundamentalsatz der Zahlentheorie):
Every integer n has a *unique prime factor decomposition* (in German: *eindeutige Primfaktorzerlegung*):

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$$

If, furthermore, $p_1 < p_2 < \ldots < p_r$ this decomposition is called the *canonical prime factor decomposition* (in German: *kanonische Primfaktorzerlegung*) of n.

(For a discussion of the basic concepts and for the proofs see for instance [Ziegenbalg 2002]).

Example in *Mathematica:*

```
FactorInteger[144000]
```

```
{{2, 7}, {3, 2}, {5, 3}}
```

Check:

$$2^7 * 3^2 * 5^3$$

```
144000
```

Remark: For the problem of factoring an integer (presently) no efficient algorithm is known. Factoring large numbers takes vast amounts of time. The RSA-method of public key cryptography heavily depends on this fact.

Theorem: Let n be an integer with the above unique prime factor decomposition.
Then $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_r + 1) \cdot$

Proof: See for instance [Ziegenbalg 2002].

Theorem: The arithmetic function $\tau: n \to \tau(n)$ is multiplicative; i.e. if a and b are relatively prime then $\tau(a \cdot b) = \tau(a) \cdot \tau(b)$.

Proof: Exercise (hint: use the unique prime factor decomposition of a, b and $a \cdot b$).

A *remark*: Divisors appear in "pairs": For any divisor d of n one has

$$n = d \cdot d_1 \qquad (*)$$

where d_1 is the divisor paired with d.
(This includes the case $d = d_1$ if n is a square number and $d = \sqrt{n}$.)

When d "runs through" all the divisors of n, then so does d_1. Therefore

$$\prod_{d \mid n} d = \prod_{d \cdot d_1 = n} d_1.$$

Next, we consider the equation

$$n = d \cdot d_1$$

in the process of d running through all the $\tau(n)$ divisors of n. Multiplying all the left hand sides and all the right hand sides of equation (*) we get

$$n^{\tau(n)} = \left(\prod_{d \mid n} d\right) \cdot \left(\prod_{d \cdot d_1 = n} d_1\right) = \left(\prod_{d \mid n} d\right)^2.$$

Taking square roots and taking into account that all numbers under consideration are positive, we get

$$\sqrt{n^{\tau(n)}} = \prod_{d \mid n} d.$$

A *Mathematica* example

```
Sqrt[24^Tau[24]]
```

```
331776
```

```
Apply[Times, Divisors[24]]
```

```
331776
```

■ Mean Excursion

Definition: Let $X := \{x_1, x_2, ..., x_r\}$ be any finite set of numbers.
Its *arithmetic mean* (in German: *arithmetisches Mittel*) is defined as

$$m_a := (x_1 + x_2 + ... + x_r)/r$$

Its *geometric mean* (in German: *geometisches Mittel*) is defined as

$$m_g := \sqrt[r]{x_1 \cdot x_2 \cdot ... \cdot x_r}$$

Its *harmonic mean* (in German: *harmonisches Mittel*) is defined as

$$m_h := \frac{1}{\frac{1}{r}\left(\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_r}\right)}$$

Thus, the harmonic mean is the "reciprocal of the arithmetic mean of the reciprocals" (in German: Das harmonische Mittel ist der Kehrwert des arithmetischen Mittels der Kehrwerte).

```
ArithmeticMean[L_] := Apply[Plus, L] / Length[L];
GeometricMean[L_] := Apply[Times, L] ^ (1 / Length[L]);
Reciprocals[L_] := Map[Function[x, 1 / x], L];
HarmonicMean[L_] := 1 / ArithmeticMean[Reciprocals[L]]
```

```
ArithmeticMean[{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}]
```

$\frac{11}{2}$

```
% // N
```

5.5

```
GeometricMean[{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}]
```

$2^{4/5}\, 3^{2/5}\, 5^{1/5}\, 7^{1/10}$

```
% // N
```

4.52873

```
Reciprocals[{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}]
```

$\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}, \frac{1}{9}, \frac{1}{10}\right\}$

```
HarmonicMean[{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}]
```

$\frac{25200}{7381}$

```
% // N
```

3.41417

■ More basic facts on Tau and Sigma

Theorem: The geometric mean of the set of divisors of the number n is

$$m_g = \sqrt{n}$$

Proof: Let $r := \tau(n)$. Then the geometric mean considered is given by $\sqrt[r]{\prod_{d\mid n} d}$.

By equation (**) we have $\prod_{d\mid n} d = \sqrt{n^{\tau(n)}}$. Therefore

$$\sqrt[r]{\prod_{d\mid n} d} = \left(\prod_{d\mid n} d\right)^{\frac{1}{r}} = \left(\sqrt{n^r}\right)^{\frac{1}{r}} = \left((n^r)^{\frac{1}{2}}\right)^{\frac{1}{r}} = n^{r\cdot\frac{1}{2}\cdot\frac{1}{r}} = n^{\frac{1}{2}} = \sqrt{n}.$$

Theorem: For a prime power p^α the sum of its divisors is

$$\sigma(p^\alpha) = 1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}. \qquad \text{(sigma-1)}$$

Proof: The theorem follows immediately from the fact that for any prime p the divisors of p^α are $\{1, p, p^2, \ldots, p^\alpha\}$.

Example in *Mathematica*:

```
Divisors[3^4]
```

```
{1, 3, 9, 27, 81}
```

Corollary: If p is a prime then $\sigma(p) = \frac{p^{1+1}-1}{p-1} = p + 1$. (sigma-2)

Corollary: $\sigma(2^\alpha) = \frac{2^{\alpha+1}-1}{2-1} = 2^{\alpha+1} - 1$.
(sigma-3)

Theorem: The arithmetic function $\sigma: n \to \sigma(n)$ is multiplicative; i.e. if a and b are relatively prime then

$$\sigma(a\cdot b) = \sigma(a)\cdot\sigma(b).$$
(sigma-4)

Proof: Let $n = a\cdot b$ where a and b are relatively prime. Since a and b are relatively prime any divisor d of n must have the form

$$d = a_i\cdot b_i \qquad (*)$$

where a_i is a divisor of a and b_i is a divisor of b.
Let $1, a_1, a_2, \ldots, a$ be the divisors of a and $1, b_1, b_2, \ldots, b$ the divisors of b.
Then $\sigma(a) = 1 + a_1 + a_2 + \ldots + a$ and $\sigma(b) = 1 + b_1 + b_2 + \ldots + b$.
Let us fix some a_i and in equation (*) consider all divisors d of n having the form $d = a_i\cdot b_j$ where b_j runs throug the divisors of b. Their sum is

$a_i \cdot (1 + b_1 + b_2 + \ldots + b) = a_i \cdot \sigma(b).$

Next, by taking this sum for all possible values of a_i (i.e. for all divisors a_i of a) one obtains the total sum of all divisors of n

$\sigma(n) = \sigma(a \cdot b) = 1 \cdot \sigma(b) + a_1 \cdot \sigma(b) + a_2 \cdot \sigma(b) + \ldots + a \cdot \sigma(b) = \sigma(a) \cdot \sigma(b).$

Excercise: Show the "mechanics" of this proof in detail by studying the example $210 = 6 \cdot 35$ in detail.

```
Divisors[210]
```

```
{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210}
```

```
Divisors[6]
```

```
{1, 2, 3, 6}
```

```
Divisors[35]
```

```
{1, 5, 7, 35}
```

```
Outer[List, Divisors[6], Divisors[35]]
```

```
{{{1, 1}, {1, 5}, {1, 7}, {1, 35}}, {{2, 1}, {2, 5}, {2, 7}, {2, 35}},
 {{3, 1}, {3, 5}, {3, 7}, {3, 35}}, {{6, 1}, {6, 5}, {6, 7}, {6, 35}}}
```

```
Flatten[%, 1]
```

```
{{1, 1}, {1, 5}, {1, 7}, {1, 35}, {2, 1}, {2, 5}, {2, 7}, {2, 35},
 {3, 1}, {3, 5}, {3, 7}, {3, 35}, {6, 1}, {6, 5}, {6, 7}, {6, 35}}
```

```
CartesianProduct[L1_, L2_] :=
 Flatten[Outer[List, L1, L2], 1]
```

```
CartesianProduct[Divisors[6], Divisors[35]]
```

```
{{1, 1}, {1, 5}, {1, 7}, {1, 35}, {2, 1}, {2, 5}, {2, 7}, {2, 35},
 {3, 1}, {3, 5}, {3, 7}, {3, 35}, {6, 1}, {6, 5}, {6, 7}, {6, 35}}
```

```
Map[Function[x, Apply[Times, x]], %]
```

```
{1, 5, 7, 35, 2, 10, 14, 70, 3, 15, 21, 105, 6, 30, 42, 210}
```

```
Apply[Plus, %]
```

```
576
```

```
(1 + 2 + 3 + 6) * (1 + 5 + 7 + 35)
```

```
576
```

```
1 * (1 + 5 + 7 + 35) + 2 * (1 + 5 + 7 + 35) + 3 * (1 + 5 + 7 + 35) + 6 * (1 + 5 + 7 + 35)
```

```
576
```

```
1 + 2 + 3 + 5 + 6 + 7 + 10 + 14 + 15 + 21 + 30 + 35 + 42 + 70 + 105 + 210
```

```
576
```

```
Sigma[210]
```

```
576
```

```
Map[Function[x, Apply[Times, x]],
 CartesianProduct[Divisors[6], Divisors[35]]]
```

```
{1, 5, 7, 35, 2, 10, 14, 70, 3, 15, 21, 105, 6, 30, 42, 210}
```

```
Sort[%]
```

```
{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210}
```

```
Divisors[210]
```

```
{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210}
```

```
% == %%
```

```
True
```

Let us show by a suitable example that the argument in the proof of the previous theorem is not valid if a and b are not relatively prime. We will study, for instance, the example $90 = 6 \cdot 15$.

```
Sigma[90]
```

```
234
```

```
Sigma[6]
```

```
12
```

```
Sigma[15]
```

```
24
```

```
Sigma[6] * Sigma[15]
```

```
288
```

```
Divisors[90]
```

```
{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90}
```

```
Divisors[6]
```

```
{1, 2, 3, 6}
```

```
Divisors[15]
```

```
{1, 3, 5, 15}
```

```
(1 + 2 + 3 + 6) * (1 + 3 + 5 + 15)
```

```
288
```

```
CartesianProduct[Divisors[6], Divisors[15]]
```

```
{{1, 1}, {1, 3}, {1, 5}, {1, 15}, {2, 1}, {2, 3}, {2, 5}, {2, 15},
 {3, 1}, {3, 3}, {3, 5}, {3, 15}, {6, 1}, {6, 3}, {6, 5}, {6, 15}}
```

```
Map[Function[x, Apply[Times, x]], %]
```

```
{1, 3, 5, 15, 2, 6, 10, 30, 3, 9, 15, 45, 6, 18, 30, 90}
```

```
Sort[%]
```

```
{1, 2, 3, 3, 5, 6, 6, 9, 10, 15, 15, 18, 30, 30, 45, 90}
```

```
Apply[Plus, %]
```

```
288
```

```
1 + 2 + 3 + 5 + 6 + 9 + 10 + 15 + 18 + 30 + 45 + 90
```

```
234
```

Analysis: $90 = 6 \cdot 15$:
Divisors of 6: 1, 2, 3, 6
Divisors of 15: 1, 3, 5, 15
Not every divisor d of 90 can uniquely be wirtten in the form $d = a \cdot b$ with $a \mid 6$ and $b \mid 15$.
For instance the divisor 3 can be written as $3 = 1 \cdot 3 = 3 \cdot 1$.
Thus, for instance, the divisor 3 of 90 is counted twice in the product (1+2+3+6)*(1+3+5+15).

Theorem: Let n be an integer with the unique prime factor decomposition

$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_r}^{\alpha_r}$$

then

$$\sigma(n) = \sigma({p_1}^{\alpha_1}) \cdot \sigma({p_2}^{\alpha_2}) \cdot \ldots \cdot \sigma({p_r}^{\alpha_r})$$

and hence

$$\sigma(n) = \frac{{p_1}^{\alpha_1+1}-1}{p_1-1} \cdot \frac{{p_2}^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \frac{{p_r}^{\alpha_r+1}-1}{p_r-1}.$$

Proof: By induction and the previous theorems.

Examples in *Mathematica*:

```
FactorInteger[144000]
```

```
{{2, 7}, {3, 2}, {5, 3}}
```

```
Sigma[144000]
```

```
517140
```

$$\frac{2^{7+1}-1}{2-1} * \frac{3^{2+1}-1}{3-1} * \frac{5^{3+1}-1}{5-1}$$

```
517140
```

■ Euler's φ-function

Theorem: The Euler φ-function is multiplicative.

Proof: See [Ziegenbalg 2002]

Theorem: If p is a prime then $\varphi(p) = p - 1$.

Proof: obvious

Theorem: If p is a prime then for any integer α

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1) = p^\alpha \cdot \left(1 - \frac{1}{p}\right).$$

Proof: See [Ziegenbalg 2002]

Theorem: Let n be an integer with the unique prime factor decomposition

$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_r}^{\alpha_r}.$$

Then

$$\varphi(n) = \varphi({p_1}^{\alpha_1}) \cdot \varphi({p_2}^{\alpha_2}) \cdot \ldots \cdot \varphi({p_r}^{\alpha_r})$$

and therefore

$$\varphi(n) = {p_1}^{\alpha_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot {p_2}^{\alpha_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot {p_r}^{\alpha_r} \cdot \left(1 - \frac{1}{p_r}\right)$$

and finally

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right)$$

Proof: See [Ziegenbalg 2002]

Examples in *Mathematica*:

```
EulerPhi[144000]
```

```
38400
```

```
FactorInteger[144000]
```

```
{{2, 7}, {3, 2}, {5, 3}}
```

$$2^7 * \left(1 - \frac{1}{2}\right) * 3^2 * \left(1 - \frac{1}{3}\right) * 5^3 * \left(1 - \frac{1}{5}\right)$$

```
38400
```

```
TableForm[
 Join[
  {{"n", "Phi"}},
  {{"---", "---"}},
  Table[{n, EulerPhi[n]}, {n, 2, 20}]]]
```

```
n       Phi
---     ---
2       1
3       2
4       2
5       4
6       2
7       6
8       4
9       6
10      4
11      10
12      4
13      12
14      6
15      8
16      8
17      16
18      6
19      18
20      8
```

Theorem ("φ *summation formula*"): For any integer n the following equation holds: $\sum_{d \mid n} \varphi(d) = n$.
(In this sum, $d = n$ has to be counted, too).

Proof: See [Ziegenbalg 2002, page 90]

Example in *Mathematica*:

```
PhiSummation[n_] :=
 For[
  (phisum = 0; d = 1),
  d <= n,
  d = d + 1,
  (phisum = phisum + If[Mod[n, d] == 0, EulerPhi[d], 0];
   If[verbose && Mod[n, d] == 0,
    Print[d, "    ", EulerPhi[d], "    ", phisum]
   ];
   If[d == n, Return[phisum]] ) ]
```

```
General::spell1 :
 Possible spelling error: new symbol name "verbose" is similar to existing symbol "Verbose". Mehr…
```

```
verbose = True;
Print[
  TableForm[{"d", "Phi", "phisum-continued"}, TableDirections → Row]];
PhiSummation[
 12]
```

```
d  Phi  phisum-continued

1    1    1

2    1    2

3    2    4

4    2    6

6    2    8

12    4    12

12
```

■ Perfect numbers

Let us take a closer look at the function σ_0 summing up the "aliquot parts".

```
DisplayForm[
 GridBox[
  Join[
   {{"n", "Sigma0", "Char"}},
   {{"---", "------", "----"}},
   Table[{
     n,
     Sigma0[n],
     Which[
      Sigma0[n] < n, " < ",
      Sigma0[n] == n, " = ",
      Sigma0[n] > n , " > "]
    }, {n, 2, 30}]],
  ColumnAlignments → {Right, Right, Left}, ColumnSpacings → 2]]
```

n	Sigma0	Char
---	------	----
2	1	<
3	1	<
4	3	<
5	1	<
6	6	=
7	1	<
8	7	<
9	4	<
10	8	<
11	1	<
12	16	>
13	1	<
14	10	<
15	9	<
16	15	<
17	1	<
18	21	>
19	1	<
20	22	>
21	11	<
22	14	<
23	1	<
24	36	>
25	6	<
26	16	<
27	13	<
28	28	=
29	1	<
30	42	>

As the examples show, the value of $\sigma_0(n)$ can be less than, equal to or greater than n.

Definition: The number n is called

deficient if $\sigma_0(n) < n$

perfect if $\sigma_0(n) = n$
abundant if $\sigma_0(n) > n$

In his book *The Elements* Euclid considered the process of continuously doubling the unit and summing up these numbers:

$1 + 2 = 3$
$1 + 2 + 4 = 7$
$1 + 2 + 4 + 8 = 15$
$1 + 2 + 4 + 8 + 16 = 31$

As these examples show, the sum can or cannot be prime.

Theorem (Euclid, The Elements, Book IX, Proposition 36): If as many numbers as we please beginning from a unit are set out continuously in double proportion until the sum of all becomes prime, and if the sum multiplied into the last makes some number, then the product is perfect.

Translation into modern terminology:
If $1 + 2 + 2^2 + 2^3 + ... + 2^n$ is prime then $(1 + 2 + 2^2 + 2^3 + ... + 2^n) \cdot 2^n$ is perfect.

In other words: If the number $2^{n+1} - 1$ is prime then $(2^{n+1} - 1) \cdot 2^n$ is perfect.

Some examples:

```
T1[n_] := Table[2^k, {k, 0, n}]
```

```
T1[10]
```

```
{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024}
```

```
T2[n_] := Table[T1[k], {k, 1, n}]
```

```
T2[10]
```

```
{{1, 2}, {1, 2, 4}, {1, 2, 4, 8}, {1, 2, 4, 8, 16}, {1, 2, 4, 8, 16, 32},
 {1, 2, 4, 8, 16, 32, 64}, {1, 2, 4, 8, 16, 32, 64, 128},
 {1, 2, 4, 8, 16, 32, 64, 128, 256}, {1, 2, 4, 8, 16, 32, 64, 128, 256, 512},
 {1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024}}
```

```
DisplayForm[
 GridBox[
  Table[
   {k,
    T1[k],
    Apply[Plus, T1[k]],
    PrimeQ[Apply[Plus, T1[k]]]},
   {k, 1, 10}], ColumnAlignments → {Right, Left, Right, Left}]]
```

```
 1  {1, 2}                                             3  True
 2  {1, 2, 4}                                          7  True
 3  {1, 2, 4, 8}                                      15  False
 4  {1, 2, 4, 8, 16}                                  31  True
 5  {1, 2, 4, 8, 16, 32}                              63  False
 6  {1, 2, 4, 8, 16, 32, 64}                         127  True
 7  {1, 2, 4, 8, 16, 32, 64, 128}                    255  False
 8  {1, 2, 4, 8, 16, 32, 64, 128, 256}               511  False
 9  {1, 2, 4, 8, 16, 32, 64, 128, 256, 512}         1023  False
10  {1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024}   2047  False
```

Excercise: Show that for any integer n the following equation holds

$$1 + 2^1 + 2^2 + ... + 2^{n-1} = 2^n - 1.$$

Excercise: Show

(i) $$a^n - b^n = (a-b) \cdot (a^{n-1} + a^{n-2} \cdot b + a^{n-3} \cdot b^2 + ... + a^2 \cdot b^{n-3} + a \cdot b^{n-2} + b^{n-1})$$

(ii) $$a^{k \cdot m} - b^{k \cdot m} = (a^m - b^m) \cdot \left(a^{(k-1) \cdot m} + a^{(k-2) \cdot m} \cdot b^m + a^{(k-3) \cdot m} \cdot b^{2 \cdot m} + ... + a^{2 \cdot m} \cdot b^{(k-3) \cdot m} + a^m \cdot b^{(k-2) \cdot m} + b^{(k-1) \cdot m}\right)$$

Hint: Expand the products and write the results systematically in the form of a twodimensional table.

Corollary: If the integer n is composite then $2^n - 1$ is not a prime.

Proof: Let $n = k \cdot m$ (with $k > 1$, $m > 1$). Then by the last excercise

$$2^n - 1 = 2^{k \cdot m} - 1 = (2^m - 1) \cdot \left(2^{(k-1) \cdot m} + 2^{(k-2) \cdot m} + ... 2^{2 \cdot m} + 2^m + 1\right)$$

and $2^n - 1$ is composite.

Corollary: For $2^n - 1$ to be a prime it is necessary that n is a prime.

Primes of the form $2^n - 1$ were studied by Marin Mersenne (1588-1648), a French Franciscan friar (i.e. a monk; etymology: friar - French: frère - German: Bruder).

```
TableForm[
 Table[{Prime[n], 2^Prime[n] - 1, PrimeQ[(2^Prime[n]) - 1]}, {n, 1, 20}]]
```

2	3	True
3	7	True
5	31	True
7	127	True
11	2047	False
13	8191	True
17	131071	True
19	524287	True
23	8388607	False
29	536870911	False
31	2147483647	True
37	137438953471	False
41	2199023255551	False
43	8796093022207	False
47	140737488355327	False
53	9007199254740991	False
59	576460752303423487	False
61	2305843009213693951	True
67	147573952589676412927	False
71	2361183241434822606847	False

Definition: If a number of the form $2^n - 1$ is prime then it is called a *Mersenne prime*.

Remark: Mersenne primes are good candidates in the search for prime number records.
Some interesting facts on primes and in particular Mersenne primes are on the following web sites:

http://www.utm.edu/research/primes/largest.html#biggest
http://www.mersenne.org/prime.htm

The five largest primes known March 2002 are the following Mersenne primes:

no.	prime	digits	year
1	$2^{13466917} - 1$	4053946	2001
2	$2^{6972593} - 1$	2098960	1999
3	$2^{3021377} - 1$	909526	1998
4	$2^{2976221} - 1$	895932	1997
5	$2^{1398269} - 1$	420921	1996

They were found through the GIMPS-project (GIMPS: Great Internet Mersenne Prime Search).

We recall **Euclid's Theorem**, The Elements, Book IX, Proposition 36 (in modern terminology):
If the number $2^{n+1} - 1$ is prime then $(2^{n+1} - 1) \cdot 2^n$ is perfect.

Proof: Let $a := (2^{n+1} - 1) \cdot 2^n$ and let $q := 2^{n+1} - 1$ be a Mersenne prime.
Because of the multiplicativity of the σ function we have

$$\sigma(a) = \sigma((2^{n+1} - 1) \cdot 2^n) = \sigma(2^{n+1} - 1) \cdot \sigma(2^n) = \sigma(q) \cdot \sigma(2^n)$$

Because q is prime $\sigma(q) = q + 1$ and by formula (sigma-3) $\sigma(2^n) = 2^{n+1} - 1$.
Hence
$$\sigma(a) = (q+1)\cdot(2^{n+1}-1) = 2^{n+1}\cdot(2^{n+1}-1) = 2\cdot(2^n\cdot(2^{n+1}-1)) = 2\cdot a$$
and a is perfect.

The following table shows the first perfect numbers (6, 28, 496, 8128, ...) obtained by applying Euclid's Theorem (instead of brute force).

```
TableForm[
 Table[{
   n,
   Prime[n],
   2^Prime[n] - 1,
   If[PrimeQ[(2^Prime[n]) - 1], (2^(Prime[n] - 1)) * (2^Prime[n] - 1)]},
  {n, 1, 20}]]
```

1	2	3	6
2	3	7	28
3	5	31	496
4	7	127	8128
5	11	2047	Null
6	13	8191	33550336
7	17	131071	8589869056
8	19	524287	137438691328
9	23	8388607	Null
10	29	536870911	Null
11	31	2147483647	2305843008139952128
12	37	137438953471	Null
13	41	2199023255551	Null
14	43	8796093022207	Null
15	47	140737488355327	Null
16	53	9007199254740991	Null
17	59	576460752303423487	Null
18	61	2305843009213693951	2658455991569831744654692615953842176
19	67	147573952589676412927	Null
20	71	2361183241434822606847	Null

By their algebraic form, all of the perfect numbers described by Euclid's theorem (above) are even. The following theorem shows that there are no other even perfect numbers.

Theorem: Every perfect number is of the type $(2^{n+1} - 1)\cdot 2^n$ with $2^{n+1} - 1$ being a prime.

Proof: Let a be an even perfect number. As an even number a can be written in the form
$$a = q\cdot 2^s \qquad (\text{with} \quad s > 0) \qquad (*)$$
with q being an odd number. Since q and 2^s are relatively prime
$$\sigma(a) = \sigma(q\cdot 2^s) = \sigma(q)\cdot\sigma(2^s) = \sigma(q)\cdot(2^{s+1} - 1).$$
Since a is perfect
$$\sigma(a) = 2\cdot a = q\cdot 2^{s+1}$$
and hence

$\sigma(q) \cdot (2^{s+1} - 1) = q \cdot 2^{s+1}.$

Using the function σ_0 (summing up only the proper divisors) the last equation reads

$(\sigma_0(q) + q) \cdot (2^{s+1} - 1) = q \cdot 2^{s+1}.$

Hence

$\sigma_0(q) \cdot (2^{s+1} - 1) = q.$

(**)

This equation implies that $d = \sigma_0(q)$ is a proper divisor of q. But $\sigma_0(q)$ is the sum of all proper divisors of q (including d). This is only possible if $d = \sigma_0(q) = 1$. Hence q is a number with 1 as its only proper divisor. This means that q is a prime. Finally, by equation (**)

$q = 2^{s+1} - 1$

and q ist a Mersenne prime.

Remark: It is unknown if there are any odd perfect numbers.

Exercises: Show that

(i) a prime number is always deficient
(ii) a prime power is always deficient
(iii) any divisor of a deficient number is deficient
(iv) any divisor of a perfect number is deficient
(v) any multiple of an abundant number is abundant
(vi) any multiple of a perfect number is abundant

Remark: For certain abundant numbers the sum of their proper divisors may turn out to be a multiple of the number itself. For example: $\sigma_0(120) = 2 \cdot 120.$

```
Sigma0[120]
```

```
240
```

Definition: The number a is called *multiply perfect* if $\sigma_0(a) = k \cdot a$ for some integer k. The integer k is called the *class* of the multiply perfect number a.
For an historically oriented discussion of multiply perfect numbers see [Ore 1948, p. 95 ff].

■ Amicable numbers

Definition: Two integers a and b are called *amicable numbers* (in German: befreundete Zahlen) if each of them is composed of the aliquot parts of the other; i.e. if

$\sigma_0(a) = b$ and $\sigma_0(b) = a.$

Example: The numbers 220 and 284 are a pair of amicable numbers.

```
Sigma0[220]
```

```
284
```

```
Sigma0[284]
```

```
220
```

Exercise: Let a and b be amicable numbers. Show that

$$\sigma(a) = \sigma(b) = a + b.$$

For an historically oriented discussion of amicable numbers and their numerology see [Ore 1948, p. 95 ff].

Remark: The perfect numbers can be characterized as the *self-amicable* numbers.

■ A short excursion into Mathematica programming

■ Factorization

Let n be an integer with the unique prime factor decomposition

$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_r}^{\alpha_r}$$

Then the function call

```
FactorInteger[144000]
```

will result in a list

```
L = {{2,7},{3,2},{5,3}}
```

```
L = FactorInteger[144000]
```

```
{{2, 7}, {3, 2}, {5, 3}}
```

The following functions **P** (for "power") and **ToNumber** will reverse this.

```
P[L2_] := L2[[1]]^L2[[2]]        (* where  L2={a,b} *)
```

```
P[{3, 4}]
```

```
81
```

```
Map[P, L]
```

```
{128, 9, 125}
```

```
Apply[Times, Map[P, L]]
```

```
144000
```

```
ToNumber[PFL_] := Apply[Times, Map[P, PFL]]
```

```
ToNumber[{{2, 7}, {3, 2}, {5, 3}}]
```

```
144000
```

Some test runs

```
n = 3^5 * 5^2 * 7^4 * 17^7 * 29^5
```

```
12276395786208460771775
```

```
FactorInteger[n]
```

```
{{3, 5}, {5, 2}, {7, 4}, {17, 7}, {29, 5}}
```

```
ToNumber[%]
```

```
12276395786208460771775
```

```
n == %
```

```
True
```

```
Test[n_] :=
 (Print[n];
  Print[FactorInteger[n]];
  Print[ToNumber[FactorInteger[n]]];
  Print[n == ToNumber[FactorInteger[n]]])
```

```
Test[27382383980902933847389402932839238O3339]
```

```
2738238398090293384738940293283923803339
```

```
{{3, 2}, {101, 1}, {27094259, 1},
 {1111808768878583244499371466669, 1}}
```

```
2738238398090293384738940293283923803339
```

```
True
```

```
TestSeries[k_] := Do[(
   Print["Test Nr.: ", i];
   Test[Random[Integer, {10^20, 10^30}]];
   Print["----------------"] ), {i, 1, k}]
```

```
TestSeries[5]
```

```
Test Nr.: 1
```

```
624595599706983855659998421674
```

```
{{2, 1}, {23, 2}, {391199, 1}, {1509091304361317293147, 1}}
```

```
624595599706983855659998421674
```

```
True
```

```
----------------
```

```
Test Nr.: 2
```

```
767415328422532292208878597029
```

```
{{11, 1}, {1367, 1}, {137119, 1},
 {2198201, 1}, {9736891, 1}, {17389373, 1}}
```

```
7674153284225322922088785970 29
```

```
767415328422532292208878597029
True
----------------
Test Nr.: 3
2893004307455464924465456831
{{67, 1}, {137279, 1}, {314535863227383749867, 1}}
2893004307455464924465456831
True
----------------
Test Nr.: 4
760806382775482402632696532442
{{2, 1}, {123397715236123, 1}, {3082740962098327, 1}}
760806382775482402632696532442
True
----------------
Test Nr.: 5
557242771260865124466434858345
{{5, 1}, {11, 4}, {373, 1}, {20407737837860117909233, 1}}
557242771260865124466434858345
True
----------------
```

■ Perfect Numbers implemented in *Mathematica*

```
PerfectNumbers[alist_] := Select[alist, 2 # == Plus @@ Divisors[#] &]
PerfectNumbers[Range[9999]]
{6, 28, 496, 8128}
PerfectNumbers2[alist_] := Select[alist, Function[x, 2 * x == Sigma[x]]]
PerfectNumbers2[Range[10000]]
{6, 28, 496, 8128}
```

■ Some Utilities

Table schemes

```
DisplayForm[
 GridBox[
  Join[
   {{"n", "Phi", "Tau", "Sigma0", "Char"}},
   {{"---", "---", "---", "------", "----"}},
   Table[{
     n,
     EulerPhi[n],
     Tau[n],
     Sigma0[n],
     Which[
      n > Sigma0[n], "deficient",
      n == Sigma0[n], "perfect",
      n < Sigma0[n], "abundant"]
    }, {n, 2, 30}]],
  ColumnAlignments → {Right, Right, Right, Right, Left},
  ColumnSpacings → 2]]
```

n	Phi	Tau	Sigma0	Char
---	---	---	------	----
2	1	2	1	deficient
3	2	2	1	deficient
4	2	3	3	deficient
5	4	2	1	deficient
6	2	4	6	perfect
7	6	2	1	deficient
8	4	4	7	deficient
9	6	3	4	deficient
10	4	4	8	deficient
11	10	2	1	deficient
12	4	6	16	abundant
13	12	2	1	deficient
14	6	4	10	deficient
15	8	4	9	deficient
16	8	5	15	deficient
17	16	2	1	deficient
18	6	6	21	abundant
19	18	2	1	deficient
20	8	6	22	abundant
21	12	4	11	deficient
22	10	4	14	deficient
23	22	2	1	deficient
24	8	8	36	abundant
25	20	3	6	deficient
26	12	4	16	deficient
27	18	4	13	deficient
28	12	6	28	perfect
29	28	2	1	deficient
30	8	8	42	abundant