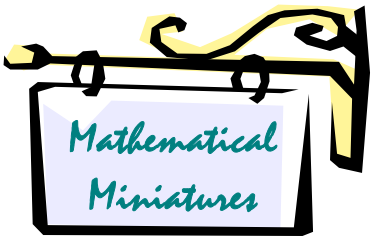

Gottfried Helms - Univ Kassel *12 - 2006*

Exponential diophantine problems: The power of cyclic subgroups

Abstract:

A notational (and conceptional) framework for discussion of exponential diophantine problems in terms of order of cyclic subgroups modulo a prime is presented. Some examples are given. We just express some know problems differently and in a coherent framework, we do not primarily attempt to arrive at new results.

Relevant aspects are:

- *modular arithmetic*
- *Eulers phi() or "totient"-function*
- *exponential equations*
- *the "little theorem of Fermat"*
- *the prime-factorization of an expression*

Note: this is still a manuscript partly in a draft state only for the support of a discussion

Gottfried Helms
Version : 12.10.2016 prev: 5.10; 28.07.2012 17:42 , ...initial: 2006

Contents:

1 Introduction and basic definitions/notations

1.1 Intro

The considerations in the current article were initially triggered by the study of the functions

(1.1.1) $f_{b,a}(n) = b^n - a^n$
$g_{b,a}(n) = b^n + a^n$

modulo some prime p, and subsequently more generally by their complete primefactorizations. For instance in terms of the question:

given a pair of "bases" a,b find the relation of p and n such that

$$b^n - a^n \equiv 0 \pmod{p} \qquad \text{//for some prime p}$$

or more explicite

given a pair of "bases" a,b find an expression for e_k depending on n in

$$b^n - a^n = \prod_{p_k \in \mathrm{Primes}} p_k^{e_k}$$

Looking at modularity with respect to some primes or to the complete primefactorization where n is a variable parameter, we may call these an *exponential diophantine problem*.

Similar other questions in that area of exponential diophantine problems are sometimes successfully formulated in terms of the *order of the multiplicative cyclic subgroup modulo a prime p*[1]. So I got up with the idea to develop a common notational framework for a unified formulation of such problems: if some problem could be answered looking at it *modulo* the prime p_1 and another problem *modulo* p_2 and p_3, then why not use a formalism which principally *refers to all primes* and can then be focused appropriately according to a current problem?

The following treatize is only concerned with the presentation of such a formalism and just a couple of rather immediate implications. I don't attempt to find some special new solutions. Rather I'm looking at some old classic problems with that "new glasses" developed here – and I find some very nice appeal in that unified view.

In general in the following **I'll look at the function $f_{b,1}(n)$** rather than at the more general one $f_{b,a}(n)$ and leave that generalization to further progress. One of the specific differences is: in $f_{b,1}(n)$ the primefactor 2 plays a special role (because $f_{b,1}(n)$ and $g_{b,1}(n)$ with $gcd(b,2)=1$ are both divisible by 2; a related effect must be taken into account for $f_{b,a}(n)$ but I've not yet looked at this more than cursory.

Two *ad hoc* introduced notations are useful for problems of wider area too: the idea of the *Iverson-brackets*[2], which means to introduce some boolean *if*-condition as numerical parameter into an algebraic formula. I focus here on the "*if m divides n*" – condition and "*highest power of m which divides n*"-value giving them symbols which allow algebraic manipulations in equations and formulae.

[1] see http://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n

[2] see http://en.wikipedia.org/wiki/Iverson_bracket

In the following I use also shorter forms for *f()* and *g()* because in most places I assume some constant parameters *a,b* so –where possible – I denote this as follows:

In general:

$f_{b,a}(n) = b^n - a^n$ and $g_{b,a}(n) = b^n + a^n$

If the parameter *a=1* then I abbreviate

$f_b(n) = b^n - 1$ and $g_b(n) = b^n + 1$

and if also *b=2* then I omit that parameter too:

f(n)	*means*	$f_{2,1}(n)$ *so*	$f(n) = 2^n - 1$
g(n)	*means*	$g_{2,1}(n)$ *so*	$g(n) = 2^n + 1$

By default I denote integers using the letters *n* or *m* or *x*, primes using *p*,*q*,*r*,*u* . The letters *b* and *a* are mostly used for the pair of possible bases usually having *gcd(a,b)=1*, and are meant as constant parameters in a certain formula, while *n, p* etc are meant as variable. The symbol *e* is never meant as euler's constant but refers to a variable in the exponent as well as the symbol *w* which alludes to the exponent of a wieferich (or generalized wieferich) prime.

Euler's totient functions is denoted by *φ(n)* ; I also introduce the greek letters *α* ("*alpha*"), *ß* ("beta") and *λ* ("*lambda*") for three essential functions (see 2.1 and 2.2)

1.2 Notation for "divides"

In the following the usual notation *m|n* for "*m divides n*" seems not well suited for use in the formulae under algebraic manipulations.[3] The main problem is to use the evaluation of that "*m divides n*"-condition as part of a concise algebraic formula. This was in principle introduced by K. E. Iverson in the programming language APL and was more popularized by D. Knuth using brackets around a boolean expression. This was in the same way meant to convert the boolean "*false*" "*true*" into arithmtical *0* and *1*, usable for instance as multiplicative factor.

So I introduce such a notation which also resembles the more "natural" use for the "divides" here and can be included in an algebraic formula, however still limited.

(1.2.1)
"Divisor-expression":
for n,m integer, m ≠ 0
[n : m] = 1 if m divides n,
[n : m] = 0 if m does not divide n

In long formulae I prefer also a second notation which reminds visually stronger to the aspect of division; I use a modification of the notation of a fraction:

(1.2.2) $$[n:m]=\underset{m}{\overset{n}{\sim}}$$

We can do a bit of algebra with that operation:

$$1-\underset{m}{\overset{n}{\sim}} \qquad negation$$

$$\underset{p}{\overset{n}{\sim}}\cdot\underset{q}{\overset{n}{\sim}} \qquad boolean\,AND$$

$$1-(1-\underset{p}{\overset{n}{\sim}})\cdot(1-\underset{q}{\overset{n}{\sim}}) \qquad boolean\,OR$$

but note, that usual operations as addition and multiplication of such "divides"-expressions in the manner of adapting sums or products of fractions do not make sense in general. However, at least we can use the arithmetical cancellation/expansion of numerator and denominator:

$$\underset{rq}{\overset{pq}{\sim}}=\underset{r}{\overset{p}{\sim}} \qquad cancellation$$

This is not fully compatible with *gcd(n,m)*. Assume three different primes *p,q,r*:

n = r · q	*m=p · q*
then	*[n : m] = 0*
but	*gcd(n,m) = q*

Remark: later I'll generalize that Iverson-bracket to contain also logical expressions like [b > a] ; this shall occur in sections to be written in the next version.

[3] For me that symbol is also unnatural, since I'm used to the divisor on the right side of the division-symbol, or even better, as denominator in a fraction, and I'd like to have this here too.

1.3 Notation for "valuation" (finding the exponent of a primefactor)

Consider the canonical primefactorization of a natural number n:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots \cdot p_m^{e_m}$$

Then the term "valuation"[4] means the exponent e_k of p_k , such that

$$e_k = valuation(n,p_k)$$

For shortness of notation I misuse the (curly) braces for that notation:

(1.3.1) *"valuation":*

$$\{n,p\} = e \quad \leftrightarrow \quad n = x \cdot p^e \quad where \quad \overset{x}{\underset{p}{\sim}} = 0$$

or

$$\{x \cdot p^e, p\} = e \qquad when \quad \overset{x}{\underset{p}{\sim\sim}} = 0$$

This can also be expressed differently as:

$$\{n,p\} = [n:p\,] + [n:p^2\,] + [n:p^3\,] + \ldots = \sum_{k=1}^{\inf} \overset{n}{\underset{p^k}{\sim}}$$

Example 1:

The obvious and natural application of that "valuation-braces" is in the canonical prime-factorization of a natural number n:

(1.3.2)
$$n = \prod_{p \in primes} p^{\{n,p\}}$$

Example 2:

The Fermat-/Euler-theorem, expressed in this notation looks for a base b, a prime p and $gcd(b,p)=1$ resp. $gcd(b,n)=1$ (where n is a positive integer)

(Fermat:)	$\{b^{p-1}-1\ ,\ p\} \geq 1$
(Euler:)	$\{b^{\varphi(n)}-1\ ,\ n\} \geq 1$
(Euler:)	$\{b^{\varphi(p^k)}-1\ ,\ p\} = \{b^{\varphi(p)p^{k-1}}-1\ ,\ p\} \geq k$

Example 3:

A more sophisticated form, reflecting the required divisibility of an exponent n by $\varphi(p)$ and possible higher powers of p for some examples:

$\{b^n-1\ ,\ p\}$	$= 0$	*if*	$[n : \varphi(p)] = 0$
	$\geq 1 + \{n,p\}$	*if*	$[n : \varphi(p)] = 1$

[4] as –for instance .- in the programming language for Pari/GP

If we express the *if* as algebraic expression using the arithmetical conversion of the "divides"-condition (the analogon to the Iverson-bracket) we can write for the power to which some prime *p* occurs in $f_b(n)$:

$\{b^n-1\ ,\ p\} = \underset{\varphi(p)}{\overset{n}{\sim}} \cdot (\alpha + \{n, p\})$ where $\alpha \geq 1$ and is explained below

Example for some prime *p*:

use $p=5$, then $\varphi(p)=4$

$$\{2^n - 1{,}5\} = \underset{\varphi(p)}{\overset{n}{\sim}} \cdot (1 + \{n, p\}) = \underset{4}{\overset{n}{\sim}} \cdot (1 + \{n{,}5\})$$

which means:

if *n* ***is not*** divisible by $\varphi(5)=4$, then the valuation of *p* (=*5*) in this expression is zero because $0\cdot(\dots)$ is always zero

if *n* ***is*** divisible by $\varphi(5)=4$ the valuation of *p* in that expression is $1\cdot(1+\{n,5\})$, which is at least *1* and if powers of *5* are also factors of *n*, then the exponent adds to that value.

Examples for some *n*:

$$\{2^7 - 1{,}5\} = \underset{4}{\overset{7}{\sim}} \cdot (1 + \{7{,}5\}) = 0 \cdot (\dots) = 0$$

$$\{2^4 - 1{,}5\} = \underset{4}{\overset{4}{\sim}} \cdot (1 + \{4{,}5\}) = 1 \cdot (1 + 0) = 1$$

$$\{2^{12} - 1{,}5\} = \underset{4}{\overset{12}{\sim}} \cdot (1 + \{12{,}5\}) = 1 \cdot (1 + 0) = 1$$

$$\{2^{20} - 1{,}5\} = \underset{4}{\overset{20}{\sim}} \cdot (1 + \{20{,}5\}) = 1 \cdot (1 + 1) = 2$$

2 Fermat/Euler and two residue-orientated functions

2.1 Fermat's little theorem and Euler's generalization

For the study of exponential diophantine problems Fermat's little theorem and Euler's generalization are the most elementary facts.

They imply cyclicitiness of divisibility of $f_{b,a}(n)$ and $g_{b,a}(n)$ by some prime p with respect to consecutive n and they allow to reduce a problem, for instance divisibility by some number, to a much smaller finite set of conditions. If we consider $f(n) = f_{2,1}(n)$ for some n and its divisibility by some prime, say $p=3, 5$ or 7 :

n:	0	1	2	3	4	5	6	7	8	9	10	...
f(n)	0	1	3	7	15	31	63	127	255	511	1023	...
[f(n):3]	1	0	1	0	1	0	1	0	1	0	1	...
[f(n):5]	1	0	0	0	1	0	0	0	1	0	0	...
[f(n):7]	1	0	0	1	0	0	1	0	0	1	0	...

…

then we observe periodicity with n in that divisibilities and looking at the values of the modular residues (not shown here) we may talk of "cyclicity".

The little theorem of Fermat is originally

if p is a prime and gcd(b,p)=1 then

(2.1.1) $b^p \equiv b \pmod p$

and can be translated to some other form:

if p is a prime and gcd(b,p)=1 then

(2.1.2) $b^{p-1} \equiv 1 \pmod p$

$b^{p-1} - 1 \equiv 0 \pmod p$

$b^{p-1} - 1 = x \cdot p$ // where $x \in IN$ may contain the factor p as well

$[b^{p-1} - 1 : p] = 1$

$\{b^{p-1} - 1 , p\} \geq 1$

and the generalization to

cyclicitiness : If p is a prime then from $b^{p-1} \equiv 1 \pmod p$ we have also

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

and with $n=m + k*(p-1)$ we have for every integer $k>0$

$b^n \equiv b^{m+k\cdot(p-1)} \equiv b^m b^{k*(p-1)} \equiv b^m \cdot 1 \equiv b^m \equiv b^{n \pmod{p-1}} \pmod p$

So the cycles with respect to varying n are modulo $(p-1)$ and the most interesting case is here when $m=0$ so

$b^{k\cdot(p-1)} \equiv 1 \pmod p$

$b^{k\cdot(p-1)} - 1 \equiv 0 \pmod p$

$[b^{k\cdot(p-1)} - 1 : p] = 1$

If we denote the exponent with n and let it vary, then this means: "*whenever n is divisible by (p-1), the expression is divisible by p*" and we can express this using the new notation for divisibility

$$[b^n - 1 : p] = \overset{n}{\underset{p-1}{\sim}}$$

L. Euler generalized this with his totient-function (*φ(m)*) to composite moduli *m*

(2.1.3) $b^{\varphi(m)} - 1 \equiv 0 \pmod m$ // gcd(b,m)=1

Because $\varphi(m) = m - 1$ if *m* is prime, this is indeed a generalization of the Fermat-theorem. With the same argument as above we can also write

(2.1.4) $b^{\varphi(m)\cdot k} - 1 \equiv 0 \pmod m$ or $[b^{\varphi(m)} - 1 : m] = 1$

or focusing a varying *n* in the exponent:

$$[b^n - 1 : m] = \overset{n}{\underset{\varphi(m)}{\sim}}$$

However, in the following we do not need that extension to composite moduli since we're going to consider only the explicite prime-factorizations of our expression and thus we need the moduli of primes only. Only we'll refer to the *φ*-function for more generality and/or completeness.

2.2 A little bit beyond the Fermat/Euler-theorem

The Fermat/Euler-theorem is very powerful, but in one sense it is too imprecise for our goal here where we want to establish a notation in equation-form and exact parameters for algebraic manipulation, not in qualitative conditions ("is cyclic", "divides") only. We'll need (at least) three improvements for that theorems.

a) The cycle length. The value $\varphi(p)$ as expression of the cycle-length of $f_{b,a}(n) \pmod p$ with respect to consecutive *n* is only an ***upper-bound for that cycle-length***. Usually the cycle-length is much smaller (while it is always a divisor of $\varphi(p)$)

Thus below we'll introduce a (cycle-) *length-function* $\lambda(\,)$ "*lambda*" . The value of this function is always a divisor of $\varphi(p)$ (including *1* or $\varphi(p)$) and is depending on the pair of bases in $f_{b,a}(n)$. We'll write it with *p* as index and (optional) *(b,a)* as parameters. So we will have

$$[b^{k\cdot\lambda_p(b,1)} - 1 : p] = 1$$

or

$$[b^n - 1 : p] = \overset{n}{\underset{\lambda_p(b,1)}{\sim}}$$

which is the same.

b) The Fermat/Euler-theorem states $f_b(\varphi(p)) \equiv 0 \pmod p$, but this is only ***a lower bound for the modulus p***. Sometimes we have $f_b(\varphi(p)) \equiv 0 \pmod{p^k}$ where $k>1$ (a problem studied under the notion of "fermat-quotient", see chap 4).

Thus below we'll introduce a *first-exponent-function* $\alpha()$ ("*alpha*") to be able to refer to the exact value. (Again, we'll write it with *p* as index and (optional) *(b,a)* as parameters) So we will have

$$\left\{b^{\lambda_p(b,1)}-1,\,p\right\}=\alpha_p(b,1)$$

or

$$\left[b^n-1:\,p^{\alpha_p(b,1)}\right]=\underset{\lambda_p(b,1)}{\overset{n}{\sim}}$$

Note: without change of properties, we can replace the reference to φ(p) by that to $\lambda_p(b,a)$, which we do here

For the correct handling of the primefactor *2*, which occurs if *b* is odd, we must also look at the exponent to which it occurs in $g_b(\varphi(2))$ and call this $\beta_b()$ ("beta") :

$$\left\{b^{\lambda_2}+1,2\right\}=\beta_2(b,1)$$

Note that also $\lambda_2 = 1$ for all odd *b*, and moreover $\alpha_2+\beta_2 > 2$

c) The Euler-theorem states, if applied to powers of primes,

$f_b(\varphi(p)) \equiv 0 \pmod p$

$f_b(\varphi(p)p^k) \equiv 0 \pmod{p^{k+1}}$

But similar to b) without further specification that increment of *1* in the exponent of the modulus *p* is only a ***lower bound for the increment*** *of k*. We want a reference to an exact value, especially we want to be able to do arithmetic in *k* on both sides of our equations. So we have to prove that increments of exponents for primefactors *p* in the lhs are correctly reflected on the rhs by the ***same increment***.

So we will have for odd primefactors p:

$$\{b^{\lambda_p(b,1)}-1,\,p\}=\alpha_p(b,1)$$

$$\{b^{\lambda_p(b,1)\cdot p^k}-1,\,p\}=\alpha_p(b,1)+k$$

short notation:

$$\{b^{\lambda_p}-1,\,p\}=\alpha_p$$

$$\{b^{\lambda_p\cdot p^k}-1,\,p\}=\alpha_p+k$$

and for *p=2* this needs completion using the function $\beta_2(b,1)$

In the following sections I introduce the needed functions λ ("*lambda*") and α ("*alpha*") and β ("beta") and a proof that the increment of exponents is indeed parallel.

2.3 Notation for cycle-length (Lambda-or *λ()* function)

If $gcd(b,p) = 1$, then the Fermat-/Euler-theorem describes the cyclicitiness of $f_b(n) \pmod p$ as

(2.3.1)

$$f_b(n) \equiv f_b(n \pmod{\varphi(p)}) \pmod p$$

$$\text{if } n = r + k \cdot \varphi(p)$$
$$f_b(n) \equiv f_p(r) \pmod p$$

But while this is true, the cycle-length can also be smaller; precisely it can equal a divisor of $\varphi(p)$. This is also known as "order of the multiplicative subgroup modulo p".

Example. If $b=2$ and $p=7$ we ask for $f_{2,1}(n)$ or $2^n-1 \pmod 7$ .Since $\varphi(7) = 6$ we have

$$f(6) = 2^6 - 1 \equiv 0 \pmod 7$$

which is obviously true. But already we have

$$f(3) = 2^3 - 1 \equiv 0 \pmod 7$$

and thus the cycle-length is 3 (which is also a divisor of 6).

This is called the *"order"* of the cyclic multiplicative subgroup; as function we find often th symbol $ord(n)$ To have a single symbol I introduce the function λ:

assuming $gcd(b,p)=1$

$\lambda_p(b,a)$: select the smallest $m>0$ such that $[b^m - a^m : p] = 1$

short forms

$\lambda_p(b) = \lambda_p(b,1)$

$\lambda_p = \lambda_p(2,1)$

$\lambda_p = \lambda_p(b,a)$ *if a certain (b,a) is understood in a formula the complete parenthese may be omitted*

$$\lambda_p(b,a) = m \quad \text{if } m>0$$
$$= <\text{infinity}> \quad \text{if there is no } m \text{ (because } gcd(b,p)>1)$$

I also use the notation λ_p or even only λ in a context, where the base b (or the pair b and a) is a constant parameter and the readability of the formula shall be improved.

Unfortunately the λ- definition interferes with the well known Carmichael-function of the same name, but I used it here because of its clarity (and also for personal historical reasons)

(Carmichael-function):The value of the smallest m, where, for all a with $gcd(a,n)=1$

$$a^m - 1 \equiv 0 \pmod n$$

is known as the *Carmichael λ( )-function* for the number n. In the example, $\lambda_{carmichael}(7)$ is not 3, but 6 because there is another base, $a=3$, where the smallest m satisfying the divisibility is 6:

$$3^6 - 1 \equiv 0 \pmod 7$$

so

(carmichael-lambda):

$$\lambda_{carmichael}(7) = 6$$

For the current discussion this function is too complex; we want to discuss properties of one single base b; (or a pair of bases in $f_{b,a}(n)$) so I introduce my own variant which denotes the smallest index m for a specific base b which is under discussion.

A brief aside: Primitive root

K.F. Gauss introduced the concept of a "primitive root" for a prime *p*. In the notion that we use here we fix a prime *p*, vary the base *b* in $f_b(n)$ and check the length-function for *p* resp that base *b*. If $\lambda_p(b,1) = p-1$, then we say, that "*b is a primitive root*" of *p*.

In another view we can characterize a primitve root *b* of *p* as "*b* is a *p-1*'th root of *1 (mod p)*" (and not a smaller one). A table of *r*'th roots of *1 (mod p)* , for instance *p=13*:

b^0	**b**	b^2	b^3	b^4	b^5	b^6	b^7	b^8	b^9	b^{10}	b^{11}	b^{12}
1	**1**	1										
1	**2**	4	8	3	6	12	11	9	5	10	7	1
1	**3**	9	1									
1	**4**	3	12	9	10	1						
1	**5**	12	8	1								
1	**6**	10	8	9	2	12	7	3	5	4	11	1
1	**7**	10	5	9	11	12	6	3	8	4	2	1
1	**8**	12	5	1								
1	**9**	3	1									
1	**10**	9	12	3	4	1						
1	**11**	4	5	3	7	12	2	9	8	10	6	1
1	**12**	1										
1	**0**	0										

We find a simple scheme here:

	all roots	"new roots"
1'st root	(1)	(1)
2'nd root	(1,12)	(12)
3'rd root	(1,3,9)	(3,9)
4'th root	(1,12,5,8)	(5,8)
6'th root	(1,12,3,9,4,10)	(4,10)
12'th root	(1,12,3,9,5,8,4,10,2,6,7,11)	(2,6,7,11)

Here the bases *b= (2,6,7,11)* are called "primitive roots": their consecutive powers "generate" the whole set of possible residues (*mod p*).

2.4 Notation for "*exponent at first occurrence*" (*α()* (="*alpha*")/*ß()*-function)

Another notation is that of the alpha-function *α()*. From a short inspection of the *λ*-function it may appear, that the exponent of the prime at its first occurrence:

$$f_{2,1}(3)= \quad 2^3 - 1 \equiv 0 \pmod 7$$

or

$$2^3 - 1 = x \cdot 7^1 \qquad \text{(and gcd(x,7)=1)}$$

or written in the new notation

(2.4.1) $$\{ f(3) , 7 \} = \{2^3 - 1, 7\} = \{2^{\lambda_7} - 1, 7\} = 1$$

is always *1* as in the given example the exponent of the prime *p=7*, as might have been found with a couple of further examples. But this is not always the case; for instance in

$$f_{3,1}(5) = 3^5 - 1 = 3^{\lambda_{11}(3,1)} - 1 = 2 \cdot 11^2$$

we find

$$\{ f_{3,1}(\lambda_{11}(3,1))) , 11\} = \{3^{\lambda_{11}} - 1, 11\} = 2$$

and that the primefactor *p=11* occurs already to the second power at its first occurence.

To be able to refer to this property in an algebraic formula we introduce the *α()*-function, which just expresses that exponent:

(2.4.2)

$$\alpha_p(b,a) = \{ f_{b,a}(\lambda_p(b,a)), p\} = \{b^{\lambda_p(b,a)} - a^{\lambda_p(b,a)}, p\}$$

$$\alpha_p(b,a) := 0 \qquad \text{if } gcd(b,p)>1 \text{ or } \lambda_p(b,a) = <infinity>$$

The *α*-function for primes *p* can alternatively be expressed using *φ(p)* instead of λ_p, or differently said:

$$\{ f(\varphi_p) , p\} = \{ f(\lambda_p) , p\}$$

because an increase of the valuation of *p* in $f(\lambda_p)$ can only occur on *p*'th multiples of λ_p, but since $\varphi_p < p$ cannot be such a multiple of λ_p it contains *p* to the same power.

As with the *λ*-function I'll omit the parameters for the base if obvious from context and if it saves notation. So for a given base *b*, for a prime *p* you'll find the reduced notation

(2.4.3) $$\alpha_p = \{ f_{b,a}(\lambda_p) , p\} = \{b^{\lambda_p} - a^{\lambda_p} , p\}$$

For the handling of the primefactor *p=2* when the difference of the bases *b-a* is *even* which occurs also in our standard cases when *a=1* and *b* is odd we need also the value of $g_{b,a}(\lambda_p)$ introducing the function *ß()*

(2.4.4) $$ß_p = \{ g_{b,a}(\lambda_p) , p\} = \{b^{\lambda_p} + a^{\lambda_p} , p\}$$

Because $\lambda_2(b,a)$ is always *1* in that cases (in the other cases the primefactor *2* does not occur at all) this looks like

(2.4.5) $$\alpha_2 = \{ f_{b,a}(1) , 2\} = \{b - a , 2\}$$
$$ß_2 = \{ g_{b,a}(1) , 2\} = \{b + a , 2\}$$

and we have also

(2.4.6) *either* $\alpha_2 = 1$ *and* $ß_p > 1$
or $\alpha_2 > 1$ *and* $ß_p = 1$

and thus

(2.4.7) $$\alpha_2 + ß_p > 2$$

A brief aside: Wieferich-primes:

Note, that the term "Wieferich-primes" refers to the function α_p in a special case. The definition for a wieferich prime is, translated to the current terminology,

(i)) *a prime p is called "wieferich-prime" if*
$\{2^{p-1}-1,p\} > 1$

For the current purposes it is useful to extend this:

(ii)) *a prime p is called "generalized wieferich-prime of order k" if*
$\{b^1 - a^1, p\} = 0$
and $\{ b^{p-1} - a^{p-1} , p \} = k > 1$

Again we can replace the exponent $p-1$ or φ_p by λ_p and write

(iii)) *a prime p is called "generalized wieferich-prime of order k"*
if $\{ f_{b,a}(1), p\} = \{ b^1 - a^1 , p \} = 0$
and $\{ f_{b,a}(\lambda_p), p\} = \{ b^{\lambda_p} - a^{\lambda_p} , p \} = \alpha_p$ *and* $\alpha_p > 1$
or shorter: a prime p is called a "generalized wieferich prime of order k"
if $\lambda_p > 1$ *and* $\alpha_p = k > 1$

(an observation:

If $\lambda_p = q$ is prime, then from $\{f(q)/f(1) ,p\} > 0$ follows,
that $p = 1 + k\cdot q$ and $f(q)$ has the form

$f(q) = (1+2kq + k^2q^2)\cdot(1+k\cdot q)^e \cdot x$
(to be continued))

2.5 Increasing powers of *p* when increasing the exponent *n*

The Fermat/Euler-theorem is quite basic and quite helpful for the numbertheoretic analysis. However, for algebraic manipulations that theorem has the drawback, that it gives only a *lower bound* for the power of a primefactor in an expression $b^n - 1$.

I'll show the problem here: the φ-formula for prime p can be extended this way:

$$b^{\varphi(p)} - 1 \equiv 0 \pmod{p}$$
$$b^{\varphi(p^k)} - 1 \equiv 0 \pmod{p^k}$$
$$b^{\varphi(p)\cdot p^{k-1}} - 1 \equiv 0 \pmod{p^k} \quad or \quad \equiv 0 \pmod{p\cdot p^{k-1}}$$

As we've seen in the paragraph on the "alpha"-function this is only a lower bound for the k on the rhs and is solved by simply introducing the alpha-function as notational reference to this property. So for some parameters

(2.5.1)
$$b^{\varphi(p)} - 1 \equiv 0 \pmod{p^{\alpha_p}}$$

with $\alpha_p > 1$ as discussed above. But moreover, the Fermat/Eulertheorem does not state explicitely, that if in

$$b^{\varphi(p)\cdot p^k} - 1 \equiv 0 \pmod{p^{\alpha_p + k}}$$

k is increased in the lhs in steps by 1, the exponent of p on the rhs increases simultaneously in steps by 1, and it is not excluded, that possibly there is a $j>0$ occuring where then

$$b^{\varphi(p)\cdot p^k} - 1 \equiv 0 \pmod{p^{\alpha_p + k + j}}$$

at some value for k. These two shortcomings are solved here.

First, we modify the Euler-formula for primes p in the following way:

$$\{b^{\varphi(p)} - 1, p\} = \alpha_p$$

because –as stated above– the exponent of p at its first occurrence may be greater than 1.

Second, it must be shown, that indeed for a certain integer $k > 0$ exactly

(2.5.2)
$$\{b^{\varphi(p)\cdot p^k} - 1, p\} = \alpha_p + k \qquad \text{// or written differently:}$$
$$b^{\varphi(p)\cdot p^k} - 1 = x\, p^{\alpha_p + k} \qquad \text{// gcd(x,p)=1}$$
$$b^{\varphi(p)\cdot p^k} = 1 + x\, p^{\alpha_p + k}$$

The general expression for the exponent of a primefactor p for odd p is then

(2.5.3) $$\mathbf{\{b^n - 1, p\} = [n : \lambda_p] \cdot (\alpha_p + \{n, p\}) \qquad for\ odd\ p,\ gcd(b,p)=1}$$

This shall be used (for odd primefactors) on the next page.

The primefactor $p=2$ needs again a special handling. We assume $f_{b,a}(n)$ and $g_{b,a}(n)$ with $a=1$ and b odd. (if b is even, then 2 does not occur at all as primefactor). We have (without given proof)

(2.5.4)
$$\{b - 1, 2\} = \alpha_2$$
$$\{b^{2^k} - 1, 2\} = \alpha_2 + k + (\beta_2 - 1) \qquad for\ k>0$$

and more compact

(2.5.5) $$\{b^{2^k} - 1, 2\} = \alpha_2 + [k>0]\,(\beta_2 - 1 + k)$$

(2.5.6) $$\{b^n - 1, 2\} = \alpha_2 + \{n, 2\} + [n:2]\,(\beta_2 - 1)$$

Or, in one formula for all primes p:

(2.5.7) $$\mathbf{\{b^n - 1, p\} = [n : \lambda_p] \cdot (\alpha_p + \{n, p\}) + [p=2][n:p]\,(\beta_p - 1)}$$

The proof (for odd primefactors) uses induction.

Assume, that this condition is true for some *k*. Then by induction we get for *k+1*

$$b^{\varphi(p)\cdot p^{k+1}} = \left(b^{\varphi(p)\cdot p^{k}}\right)^{p} = \left(1 + x\cdot p^{\alpha_p + k}\right)^{p}$$

The binomial expansion of the rhs is of course

$$1 + p\cdot x\cdot p^{\alpha_p + k} + \binom{p}{2}\cdot\left(x\cdot p^{\alpha_p + k}\right)^{2} + \binom{p}{3}\cdot\left(x\cdot p^{\alpha_p + k}\right)^{3} + \ldots + p\cdot\left(x\cdot p^{\alpha_p + k}\right)^{p-1} + \left(x\cdot p^{\alpha_p + k}\right)^{p}$$

and we can rewrite and factor out:

$$b^{\varphi(p)^{*}p^{k+1}} - 1 = p\cdot x\cdot p^{\alpha_p + k}\left[1 + \frac{\binom{p}{2}}{p}\left(x\cdot p^{\alpha_p + k}\right) + \frac{\binom{p}{3}}{p}\left(x\cdot p^{\alpha_p + k}\right)^{2} + \ldots + \left(x\cdot p^{\alpha_p + k}\right)^{p-2} + x^{p-1}\left(p^{\alpha_p + k}\right)^{p-2}\right]$$

Here, because *p* is prime the binomial-coefficients are all divisible by *p* and the relevant aspect occurs now in the shortened representation

$$b^{\varphi(p)^{*}p^{k+1}} - 1 = x\cdot p^{\alpha_p + k + 1}\cdot\left(1 + p\cdot z\right)$$

in that the rhs contains the factor *p* to the power $\alpha_p + k+1$ but not higher.

Since for the induction-start, *k=0*, we can use just the defininition α_p such that is

$$\{b^{\varphi(p)\cdot p^{0}} - 1, p\} = \alpha_p \qquad (\geq 1)$$

we finally get from this by induction

$$\begin{aligned}\{b^{\varphi(p)\cdot p^{k}} - 1, p\} &= \{b^{\varphi(p)\cdot p^{0}} - 1\ ,\ p\} + k\\ &= \{b^{\varphi(p)} - 1\ ,\ p\} + k\\ &= \alpha_p + k\end{aligned}$$

as desired.

(End of proof)

Then we have always the exact expression for the exponent of a primefactor *p* in *f(n,b)*

(iv)) $\{b^{\varphi(p)\cdot p^{k}} - 1, p\} = \alpha_p + k$

$\{b^{x\varphi(p)\cdot p^{k}} - 1, p\} = \alpha_p + k$ // for gcd(x,p)=1

where the reference to the φ-function can also be replaced by the reference to the λ-function

(v)) $\{b^{x\,\lambda_p\cdot p^{k}} - 1, p\} = \alpha_p + k$ // for gcd(x,p)=1

and the general representation in terms of decomposition of a given *n*:

(vi)) $\{b^{n} - 1, p\} = [n{:}\,\lambda_p]\cdot(\alpha_p + \{n,p\})$

3 Applications

3.1 Simple examples of primefactor-decomposition

Example: any natural number n

The canonical primefactor-representation of a natural number *n* can now be given as

(3.1.1) $$n = \prod_{p \in primes} p^{\{n,p\}}$$

because the valuation-braces "extract" just the exponent of a so-referred prime in that canonical representation.

Example: denominator of Bernoulli-numbers/von Staudt-Clausen theorem

The denominators of the Bernoulli-numbers in their most cancelled form can be described by:

(3.1.2) $$denominator(B_n) = 2^{\tilde{\frac{n}{2}}} * \prod_{\substack{p \in odd \\ primes}} p^{\tilde{\frac{n}{p-1}}}$$

according to the von Staudt/Clausen-theorem very similar to the *n*-representation (see for instance wikipedia[5]).

3.2 The canonical primefactor-decomposition of $f_{b,1}(n)$ and $g_{b,1}(n)$

The previous can be used for the description of the canonical primefactor-decomposition of $f_{b,a}(n)$ and $g_{b,a}(n)$, because the same is valid for all primefactors. For the primefactor *2* there is one more extension to be considered, so we exclude it here from the composition-scheme (giving it the formal exponent *m*, which can be zero) and write for $f_{b,1}(n)$:

(3.2.1)
$$b^n - 1 = 2^{\alpha_2 + \tilde{\frac{n}{2}}(\beta_2 - 1 + \{n,2\})} \cdot \prod_{\substack{p \in odd \\ primes}} p^{\tilde{\frac{n}{\lambda_p}}(\alpha_p + \{n,p\})} \qquad for\ odd\ b$$
$$b^n - 1 = \prod_{\substack{p \in odd \\ primes}} p^{\tilde{\frac{n}{\lambda_p}}(\alpha_p + \{n,p\})} \qquad for\ even\ b$$

(redundant base-parameter b has been omitted and shorter indexed notation for λ and α was used)

For example, for base *b=2* we have

$$2^n - 1 = 3^{\tilde{\frac{n}{2}}(1+\{n,3\})} 5^{\tilde{\frac{n}{4}}(1+\{n,5\})} 7^{\tilde{\frac{n}{3}}(1+\{n,7\})} 11^{\tilde{\frac{n}{10}}(1+\{n,11\})} \cdots 1093^{\tilde{\frac{n}{364}}(2+\{n,1093\})} \cdots$$

where I show the first few primes as factors and also the wieferich-prime *p=1093*, which, if *n* is divisible by *364* (or *1092*), occurs even to the 2^{nd} power in the value of 2^n-*1*.

[5] https://de.wikipedia.org/wiki/Bernoulli-Zahl

Example: representation of $g_b(n)$ derived from $f_b(n)$

Since

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

we can describe the composition of $g_b(n)$ immediately. We leave the powers of 2 indeterminate, give its exponent just the name m_1 and have:

$$b^n + 1 = 2^{m_1} \cdot \frac{\prod_{p \in odd\ primes} p^{\overset{2n}{\sim}_{\lambda_p}(\alpha_p + \{2n,p\})}}{\prod_{p \in odd\ primes} p^{\overset{n}{\sim}_{\lambda_p}(\alpha_p + \{n,p\})}} \tag{3.2.2}$$

First we can put numerator and denominator together, since we have the same list of primefactors:

$$b^n + 1 = 2^{m_1} \cdot \prod_{p \in odd\ primes} p^{\overset{2n}{\sim}_{\lambda_p}(\alpha_p + \{2n,p\}) - \overset{n}{\sim}_{\lambda_p}(\alpha_p + \{n,p\})} \tag{3.2.3}$$

Next; since this is a product of odd primes only, the expression $\{2n,p\}$ and $\{n,p\}$ are equal; the valuation of an odd prime p in n is the same as in $2n$, and we can compress the above expression:

$$b^n + 1 = 2^{m_1} \cdot \prod_{p \in odd\ primes} p^{\left(\overset{2n}{\sim}_{\lambda_p} - \overset{n}{\sim}_{\lambda_p}\right)(\alpha_p + \{n,p\})} \tag{3.2.4}$$

Here the parenthese of the "divides" in the exponent is of special interest. Since if n is a multiple of λ_p then is also $2n$, the whole parenthese evaluates to zero, and the primefactor in question cannot occur in b^n+1.

This can also be seen because in

$$(b^n + 1) = 2 + (b^n - 1)$$
$$g_b(n) = 2 + f_b(n)$$

the $f_b(n)$ and $g_b(n)$-functions of the same parameters could only have 2 as common factor.

Now which primes can occur in b^n+1? Obviously only that primes, whose cycle-lengthes λ_p for the current base do ***not*** divide n ***but*** divide $2 \cdot n$, for instance those whose cyclelength is even when n is odd, and generally, whose cyclelength has one more power of 2 than n has (besides the other divisibility conditions).

For example, $g(n)=2^n+1$ has the composition:

$$2^n + 1 = 3^{(\overset{2n}{\sim}_2 - \overset{n}{\sim}_2)(1+\{n,3\})}\, 5^{(\overset{2n}{\sim}_4 - \overset{n}{\sim}_4)(1+\{n,5\})}\, 7^{(\overset{2n}{\sim}_3 - \overset{n}{\sim}_3)(1+\{n,7\})}\, 11^{(\overset{2n}{\sim}_{10} - \overset{n}{\sim}_{10})(1+\{n,11\})} \cdots 1093^{(\overset{2n}{\sim}_{364} - \overset{n}{\sim}_{364})(2+\{n,1093\})} \cdots$$

Here we can see that primefactors vanish in case their λ-value is odd, since

$[2n : \lambda_p] = [n : \lambda_p]$ if λ_p is odd

and the whole exponent vanishes then.

For the primefactor 3 we observe, that the "divides"-term in the exponent is just

$1 - [n : 2]$,

that means, it vanishes at even n and occurs at all odd n.

For the other primefactors we observe, that they occur first when n is half the cyclelength and then cyclically with their cycle-period, for example $p=11$ occurs at

$n=5, 15, 25, \ldots$.

3.3 If $b^m - a^n = d$, are there more solutions $b^{m+x} - a^{n+y} = d$?

3.3.1 Solutions of $3^n-2^m=1$ or $2^n-3^m=1$? (solved in the 13th century)

We rearrange the equations to have $f_{b,1}(n)$-expressions:

1) $3^n - 1 = 2^m$
2) $2^n - 1 = 3^m$

We have "trivial solutions" for case *1)*

n=1	*3-1=2*	*--> m=1*
n=2	*9-1 = 2^3*	*--> m=3*

and for case *2)*

n=2	*4 – 1=3*	*--> m=1*

and search for more solutions. We always formulate the primefactor-compositions of the lhs in terms of the primefactors on the rhs.

Case *1):* we consider the general relation:

$$\begin{aligned}\{3^n-1,2\} &= \alpha_2 + \overset{n}{\underset{2}{\sim}}(\beta_2 - 1 + \{n,2\}) \\ &= 1 + \overset{n}{\underset{2}{\sim}}(2-1+\{n,2\}) \\ &= 1 + \overset{n}{\underset{2}{\sim}}(1+\{n,2\})\end{aligned}$$

Because we have a distinction between even and odd n we separate this in two expressions

$$\begin{aligned} a)\quad \{3^{2n}-1,2\} &= 1 + \overset{2n}{\underset{2}{\sim}}(1+\{2n,2\}) \\ &= 3 + \{n,2\} \\ b)\quad \{3^{2n+1}-1,2\} &= 1\end{aligned}$$

From that descriptions we can reformulate *a)* and *b)* to meet our question:

$$a)\quad 3^{2n}-1 = 2^{3+\{n,2\}}$$

$$9^n - 1 = 8 \cdot 2^{\{n,2\}}$$

$$\frac{9^n-1}{8} = 2^{\{n,2\}} \qquad (\le n)$$

Because the rhs $2^{\{n,2\}} <= n$ for all n, but the lhs is always greater than n when $n>1$, the expression shows that the only solution is $n=1$ or said differently (and with more generality): "we have a contradiction if n becomes greater than some small value" (the "trivial" solutions).

$$b)\quad \{3^{2n+1}-1,2\} = 1$$

Here we see, that the primefactor *2* always occurs only to the first power, so for any $n>0$ we need additional primefactors to multiply up to the value of $3^{2n+1}-1$ and thus the formula is correct only for $n=0$.

a) and b) together give us the two only possible solutions $3^2 - 1 = 2^3$ and $3^1 - 1=2^2$

Now for the ***case 2)***

$$e_3(n) = \{2^n - 1, 3\} \overset{n}{\underset{2}{\sim}} (1 + \{n, 3\})$$

$$2^n - 1 \overset{?}{=} 3^{e_3(n)}$$

Again we have, that $3^{e_3(n)} <= n$ for all n, and only if n is a perfect power of 3 (which is required here) then we have equality. Because the lhs of the equation is exponential in n we'll have at most one solution and this is $n=1$.

Thus the only possible solution is (the trivial one) $2^1 - 1 = 3^0$

This analysis of the two possible cases disproves the possibility of neighboured perfect powers of 2 and 3 beyond "the trivial" one $3^2-2^3=1$

3.3.2 Example: $2^5 - 3^3 = 5$. Are there more solutions $2^{5+a} - 3^{3+b} = 5$?

This is a concrete example for a more general problem. We do the following ansatz

$$2^5 - 3^3 = 13 \overset{?}{=} 2^{5+a} - 3^{3+b}$$

$$3^{3+b} - 3^3 \overset{?}{=} 2^{5+a} - 2^5$$

$$\frac{3^b - 1}{2^5} \overset{?}{=} \frac{2^a - 1}{3^3}$$

and look at the conditions which this imposes on the unknown exponents b and a.

For the lhs, we know that

$$\{3^n - 1\ ,\ 2\} = 1 + [n:2](1 + \{n,2\})$$

and for this expression to equal 5 we must have that

$$1 + [b:2](1 + \{b,2\}) = 5 \qquad \text{// so b must be even}$$
$$\{b,2\} = 3$$

and b must -with any odd x- have the form

$b = 2^3 \cdot x$ and we get

$\{3^{2^3 x} - 1\ ,2\} = 5$

For the rhs, we know that

$$\{2^n - 1\ ,\ 3\} = [n:2](1 + \{n,3\})$$

and for the rhs in this equation to equal 3 we must have that

$$3 = [a:2](1 + \{a,3\}) \qquad \text{// so a must be even}$$
$$2 = \{a,3\} \qquad \text{// so a must be divisible by } 3^2$$

and a must -with any y not divisible by 3- have the form

$a = 2 \cdot 3^2 \cdot y$ and we get

$\{2^{2 \cdot 3^2 y} - 1\ ,3\} = 3$

Our basic ansatz looks now like:

$$\frac{3^{2^3 x} - 1}{2^5} \overset{?}{=} \frac{2^{2.3^2 y} - 1}{3^3}$$

The constant exponents in the numerators in each side make sure, that the numerators have the denominators exactly as factors, and no less or more of the primefactors in the

denominators are allowed to occur, so any involved x may not contain the primefactor 2, and any involved y may not contain the primefactor 3.

However, if $x,y>0$ (which we assume for a second solution) each side contains further primefactors, and in the case of existence of a solution that primefactors must be the same and their exponents must be equal.

The key of the following is to prove, that this is impossible; and the most simple case is, when either in the exponent in the lhs are more primefactors 2 or in that of the rhs are more primefactors 3 - which occurs if either x has the primefactor 2 as well as if y the primefactor 3.

We assume first, that $x=y=1$ and look at the primefactors of the lhs. We get

$lhs = (2^5\cdot)\ \ 5\cdot 41$
$rhs = (3^3\cdot)\ \ 7\cdot 19\cdot 73$

(the primefactors in parentheses are cancelled by the denominators)

We see, that the lhs and rhs are mutually missing all the primefactors of the other side, so x as well as y must be adapted such that both sides have the same primefactors.

We have

$\{2^n-1,\ \ \ 5\} = [n:\ 4]\ \ (1+\{n,5\})$
$\{2^n-1,\ \ 41\} = [n:20]\ \ (1+\{n,41\})$

so $2\cdot 3^2\cdot y$ must be divisible by the $lcm(2,9,4,20)=180=2\cdot 3^2\cdot 2\cdot 5$ so $y=10\cdot y_1$ with some y_1 not divisible by 3.

For the other side we have

$\{3^n-1,\ \ \ 7\} = [n:\ 6]\ \ (1+\{n,7\})$
$\{3^n-1,\ \ 19\} = [n:18]\ \ (1+\{n,19\})$
$\{3^n-1,\ \ 73\} = [n:12]\ \ (1+\{n,73\})$

so $2^3\cdot x$ must be divisible by the $lcm(8,6,18,12)=72$ so $x=9\cdot x_1$

Setting $x_1= y_1 = 1$ we get new sets of primefactors. We get

$lhs = (2^5\cdot)\ 5\cdot 41\ \ \ \cdot 7\cdot 19\cdot 73\ \ \ \cdot 13\cdot 37\cdot 757\cdot \ldots$ (one more)
$rhs = (3^3\cdot)\ 7\cdot 19\cdot 73\ \ \ \cdot 5\cdot 41\ \ \ \cdot 5\cdot 11\cdot 13\cdot 31\cdot 37\cdot 61\cdot 109\cdot\ 151\cdot\ 181\cdot\ 331\cdot\ 631\cdot \ldots$ (some more)

(the primefactors in parentheses are cancelled by the denominators)

If we now adapt the list of primefactors again, we get in the rhs the primefactor 757. But $\lambda_{757}(2,1)= 756 = 2^2\cdot 3^3\cdot 7$ and this means, on the rhs we get $\{2^{2\cdot 3^2\cdot 2\cdot 5\ \cdot 3\cdot 7\cdot y_3} - 1,3\} = 4$ which means that the rhs becomes divisible by 3^4 instead of 3^3, and after cancelling by the denominator we get thus one remaining primefactor 3 in the rhs.

The lhs cannot have a primefactor 3, so we have a contradiction: the lhs and rhs cannot be equal and thus we cannot have a second solution for the problem in question.

This method can simply be adapted for other configurations; practically in a software implementation we need one initializing-step which sets the valuation-formulae for some sufficient subset of first primes for the lhs and for the rhs, and then, on the k'th iteration the required x_k and y_k must be determined, then for each side the set of included primefactors, then that two sets must be joined (using the highest exponent per primefactor) and new x_{k+1} and y_{k+1} must be computed until the contradiction occurs.

3.4 Are there common factors of "iterated" Fermat-numbers 2^2^... + 1?

One occasionally asked question can immediately be answered: can b^n+1 and $b^{2^n}+1$ have common primefactors?

> If $b = 2$ and $n=2$ or any powertower of 2 then this is the question of common factors of iterated fermat numbers where a "Fermat number" F_n is defined as
>
> $F_n = 2^{2^n} + 1$

We write the primefactor-decompositions of both formulae

(3.4.1)
$$b^{2^n}+1 = \prod_{\substack{p\in odd\\ primes}} p^{\left(\begin{smallmatrix}2^{n+1}\\ \sim\\ \lambda_p\end{smallmatrix} - \begin{smallmatrix}2^n\\ \sim\\ \lambda_p\end{smallmatrix}\right)\left(\alpha_p+\{2^n,p\}\right)} \qquad b^n+1 = \prod_{\substack{p\in odd\\ primes}} p^{\left(\begin{smallmatrix}2n\\ \sim\\ \lambda_p\end{smallmatrix} - \begin{smallmatrix}n\\ \sim\\ \lambda_p\end{smallmatrix}\right)\left(\alpha_p+\{n,p\}\right)}$$

We look at the parenthese in the exponent of the first product:

we have, that (for a current prime p) λ_p must divide a perfect power of 2 and must thus itself be a perfect power of 2. To provide a value of 1 for the parenthese, it must exactly equal 2^{n+1} otherwise the whole parenthese is zero and the primefactor does not occur in the lhs.

But if now for some p its "length" is $\lambda_p = 2^{n+1}$ then it cannot at the same time be a divisor of $2n$ or even of n in the exponent of the second product since $2^{n+1} > 2\cdot n > n$ for $n>0$; so any prime p can only occur in the first or in the second expression exclusively.

We did not make an assumption about the height of the powertower $n=k$, 2^k, 2^{2^k},... , so this can easily be generalized by induction. Note also, that we did not make use of the restriction for the base $b=2$, so this is a property not only of "iterated" fermat-numbers (defined for base $b=2$)

3.5 The "chinese"-primality test

The so called "chinese"-primality test for a number n is to calculate, using $f_{2,1}(n)$ with base 2:

(3.5.1) $y = 2^{n-1} - 1 \pmod n$

If $y<>0$, then we know that n is composite. Unfortunately the converse is not true. For some n we get $y=0$ although n is not prime. Such n are called "fermat pseudo-primes" (to base 2). This imperfect prime-detection property extends to other bases coprime to n as well. However, different bases b give sometimes different results and so they may correct each other, and only if we check all bases $b<n$ we get a decisive result: if all results are 0 then n is prime.

Such pseudoprimality of n consists of two or more prime-factors whose cycle-lenghtes agree to divide $n-1$. Let $n = p\cdot q$ then, being fermat-pseudoprime, $2^{n-1}-1$ must contain those factors (among others, which are collected in the indeterminate x)

(3.5.2) $$y_2 = 2^{pq-1} - 1 = p^{\overset{\sim}{\lambda_p}\left(\alpha_p + \{pq-1,p\}\right)}\, q^{\overset{\sim}{\lambda_q}\left(\alpha_q + \{pq-1,q\}\right)}\, x$$

which can directly be reduced (since $\{pq-1,p\}=0$ and $\{pq-1,q\}=0$) to

(3.5.3) $$y_2 = 2^{pq-1} - 1 = p^{\overset{\sim}{\lambda_p}\alpha_p}\, q^{\overset{\sim}{\lambda_q}\alpha_q}\, x$$

Remember that each prime and its length-function are related by $p = k\cdot\lambda_p+1$ (and then also that $q = j\cdot\lambda_q+1$) - with some positive integers k,j - , then the "divides"-expression in the exponent $n-1 = pq-1$ at primefactor p is

$$[\,((k\,\lambda_p+1)(j\,\lambda_q+1)-1\,) : \lambda_p\,] = [\,(k\,\lambda_p\,(j\,\lambda_q+1)+j\,\lambda_q) : \lambda_p\,]$$

So p and q are contained in $2^{n-1}-1$ if $\{j\,\lambda_q, \lambda_p\}>0$ and $\{k\,\lambda_p, \lambda_q\}>0$, and this is specifically given, if $\lambda_p = \lambda_q$

Let's use two primes p, q which have λ being a multiple of 5, so $p=11$, having $\lambda_p=10$, and $q=31$, having $\lambda_q=5$. Then

(3.5.4) $$2^{pq-1} - 1 = 2^{10*30+10+30} - 1 = 11^{\overset{\sim}{10}\,1}\, 31^{\overset{\sim}{5}\,1} * x = 11*31*x$$

and indeed $\{2^{n-1}-1,11\}=1$ and $\{2^{n-1}-1,31\}=1$ and thus $\{2^{n-1}-1,n\}=1$ does not detect, that n is composite, so n is (fermat-) pseudoprime to base 2.

Actually $n=11\cdot31=341$ is also the first fermat-pseudoprime to base 2

However, using base $b=3$ we get by different cycle-lengthes λ

$pq-1=11\cdot31-1 =(10+1)(30+1)-1 = 10\cdot30 + 10 + 30 \quad (= 340)$

$\lambda_{11}(3,1)=5 \qquad \alpha_{11}(3,1)=2$
$\lambda_{31}(3,1)=30 \qquad \alpha_{31}(3,1)=1$

$$y_3 = 3^{10*30+10+30} - 1 = 11^{\overset{\sim}{5}\,2}\, 31^{\overset{\sim}{30}\,1} = 11^2 * 31^0 * x$$

and y_3 does not contain the primefactor q, and thus $\{\,3^{n-1}-1,\, n\,\}=0$; this time showing that n is not prime.

The fermat-primetest can be improved this way; however there are numbers *n* which are pseudoprime to ***all*** bases *b<n* ***where also*** *gcd(b,n)=1*. Such numbers are called "Carmichael-numbers"; the first one is *n=561*. For such numbers the actual primality-certificate based on the fermat-primality test is as expensive as a dumb trial-division.

n=561 *p=3 q=11 r=17*

base 2:

$\lambda_3(2,1) = 2$ $\alpha_3(2,1) = 1$

$\lambda_{11}(2,1) = 10$ $\alpha_{11}(2,1) = 1$

$\lambda_{17}(2,1) = 8$ $\alpha_{17}(2,1) = 1$

$f_{2,1}(561-1) = 2^{560}-1 = 3^{\tilde{}\frac{560}{2}\,1}\,11^{\tilde{}\frac{560}{10}\,1}\,17^{\tilde{}\frac{560}{8}\,1} * x = 3*11*17*x$

$\equiv 0 \pmod n$

=> pseudoprime

base 3:

$f_{3,1}(561-1)$ base 3 is not coprime with n

base 5

$\lambda_3(5,1) = 2$ $\alpha_3(5,1)=1$

$\lambda_{11}(5,1) = 5$ $\alpha_{11}(5,1)=1$

$\lambda_{17}(5,1) = 16$ $\alpha_{17}(5,1)=1$

$f_{5,1}(561-1) = 5^{560}-1 = 3^{\tilde{}\frac{560}{2}\,1}\,11^{\tilde{}\frac{560}{5}\,1}\,17^{\tilde{}\frac{560}{16}\,1} * x = 3*11*17*x$

$\equiv 0 \pmod n$

=> pseudoprime

and so on with the remaining bases smaller and coprime to *n*.

3.6 The Zsigmondy-theorem

(from wikipedia: Zsigmondy's theorem)

In number theory, Zsigmondy's theorem, named after Karl Zsigmondy, states that if $a > b > 0$ are co-prime integers, then for any natural number $n > 1$ there is a prime number p (called a primitive prime divisor) that divides $b^n - a^n$ and does not divide $b^k - a^k$ for any positive integer $k < n$, with the following exceptions:

$a = 2, b = 1$, and $n = 6$; or
$a + b$ is a power of two, and $n = 2$.

This generalizes Bang's theorem, which states that if $n>1$ and n is not equal to 6, then 2^n-1 has a prime divisor not dividing any 2^k-1 with $k<n$.

Similarly, b^n+a^n has at least one primitive prime divisor with the exception $2^3+1^3=9$

This theorem expressed in the current notation is

Let p,q,r,s,t,e be primes

Then write the primefactorizations

(3.6.1) $f_{b,a}(s) = \prod_{e:\lambda_e=1} e^{\alpha_e+\{s,e\}} \prod_{p:\lambda_p=s} p^{\alpha_p+\{s,p\}}$

(3.6.2) $f_{b,a}(t) = \prod_{e:\lambda_e=1} e^{\alpha_e+\{t,e\}} \prod_{q:\lambda_q=t} q^{\alpha_q+\{t,q\}}$

Then if we look at $f_{b,a}(s\cdot t)$ we shall not only have the product of the two single products but a new set of primefactors r whose length function is $\lambda_r = s\cdot t$:

(3.6.3) $$f_{b,a}(s\cdot t) = \prod_{e:\lambda_e=1} e^{\alpha_e+\{st,e\}} \prod_{p:\lambda_p=s} p^{\alpha_p+\{st,p\}} \prod_{q:\lambda_q=t} q^{\alpha_q+\{st,q\}} \prod_{r:\lambda_q=s\cdot t} r^{\alpha_r+\{st,r\}}$$

From the representation of $f_{b,a}(n)$ in the proposed form of primefactorization it is obvious, that if some primes p_k divide $f_{b,a}(q)$, where q is also prime, then that same primes divide composite n which contain q as factor.

(3.6.4) $$f_{b,a}(n) = f_{b,a}(q_1^{e_1}q_2^{e_2}q_3^{e_3})$$
$$= \prod_{\substack{p\in odd\\ primes}} p^{\tilde{\lambda}_p^{q_1}(\dots)} \prod_{\substack{p\in odd\\ primes}} p^{\tilde{\lambda}_p^{q_2}(\dots)} \prod_{\substack{p\in odd\\ primes}} p^{\tilde{\lambda}_p^{q_3}(\dots)}$$

contains at least the same primefactors as

$$= x * \prod_{\substack{p\in odd\\ primes}} p^{\tilde{\lambda}_p^{q_1q_2q_3}(\dots)}$$

But empirically more is true: apparently the composite n does not only produce the primefactors p_k in $f_{b,a}(n)$ according to its own primefactors q_k, but also additional primefactors p_m, which do not account to the factors of n.

This can also immediately be seen by that representation: there may exist some primefactors p_m which have a length-function equal to some partial ***product*** of the q-primefactors.

$$= x * \prod_{\substack{p\in odd\\ primes}} p_k^{\tilde{\lambda}_p^{q_1}(\dots)} \prod_{\substack{p\in odd\\ primes}} p_k^{\tilde{\lambda}_p^{q_2}(\dots)} \prod_{\substack{p\in odd\\ primes}} p_k^{\tilde{\lambda}_p^{q_3}(\dots)} \prod_{\substack{p\in odd\\ primes}} p_m^{\tilde{\lambda}_p^{q_1q_2}(\dots)} \prod_{\substack{p\in odd\\ primes}} p_m^{\tilde{\lambda}_p^{q_2q_3}(\dots)} \prod_{\substack{p\in odd\\ primes}} p_m^{\tilde{\lambda}_p^{q_1q_2q_3}(\dots)}$$

This can also be seen, if we consider, that $f_{b,a}(n)$ with n consisting of two primefactors q and r is divisible by the factors

$$b^{qr}-a^{qr} = (b-a) * x_1$$
$$= (b^q)^r-(a^q)^r = ((b^q)-(a^q)) * x_2$$
$$= (b^r)^q-(a^r)^q = ((b^r)-(a^r)) * x_3$$

where also the latter two factors can be factorized:

$$b^{qr}-a^{qr} = (b-a) * x_1$$
$$= (b^q)^r-(a^q)^r = (b-a)\,[((b^q)-(a^q))/(b-a)] * x_4$$
$$= (b^r)^q-(a^r)^q = (b-a)\,[((b^r)-(a^r))/(b-a)] * x_5$$

where the []-bracketed terms (*not an Iverson-bracket here!*) are coprime, because their (prime) exponents are different. Because of this we can still proceed and even write

(3.6.5) $$= (b^r)^q-(a^r)^q = (b-a)\,[((b^r)-(a^r))/(b-a)]\,[((b^q)-(a^q))/(b-a)] * x_6$$

Actually, Zsigmondy has proved, that this holds generally with the exception of $f_{2,1}(6)=63$ which contains only factors which are already contained in $f_{2,1}(3)$ and $f_{2,1}(2)$.

3.7 Mersenne-numbers

For the case of $(b,a)=(2,1)$ we call $f_{2,1}(n)=2^n-1$ a "mersenne-number" M_n . In a more strict usage it is required that n is in fact a prime q , which is also common. *We use the strict definition in this chapter, but shall use the non-strict definition in the chapter on "iterated Mersenne numbers".*

In the notation of cyclic-subgroup-functions this reads like:

$$M_q = 2^q - 1 = \prod_{\substack{p \in odd \\ primes}} p^{\tilde{\lambda_p}^{q}(\alpha_p + \{q,p\})} \qquad // \text{ q is prime} \tag{3.7.1}$$

More explicite,

$$2^q - 1 = 3^{\tilde{2}^{q}(1+\{q,3\})} 5^{\tilde{4}^{q}(1+\{q,5\})} 7^{\tilde{3}^{q}(1+\{q,7\})} 11^{\tilde{10}^{q}(1+\{q,11\})} \cdots 1093^{\tilde{364}^{q}(2+\{q,1093\})} \cdots \tag{3.7.2}$$

where also the Wieferich-primefactor $p=1093$ is explicitely displayed for reminding the reader of special cases.

The primefactor 2 cannot occur, so we need not consider its properties here.

Since mersenne-numbers in the strict sense are only defined for prime q, we see that only primefactors can occur, which have prime cycle-lengthes $\lambda_p=q$. (or $\lambda_p=1$ but this cannot occur since $2^1-1=1<p_k$ *for all* k)

For instance the primefactor $p=5$ cannot occur in any *strict* Mersenne-number M_q because $\lambda_p=4$ never divides any prime q, as well as $p=11$ cannot occur and others. Also the two known wieferich-primefactors $p=1093$ and $p=3511$ cannot occur, since their cycle-lengthes are $\lambda_{1093}=2^2\cdot 7\cdot 13$ and $\lambda_{3511}=3^3\cdot 5\cdot 13$ and thus not prime. So we can reduce the list of candidate primefactors to

$$2^q - 1 = 3^{\tilde{2}^{q}(1+\{q,3\})} 7^{\tilde{3}^{q}(1+\{q,7\})} 23^{\tilde{11}^{q}(1+\{q,23\})} 31^{\tilde{5}^{q}(1+\{q,31\})} 47^{\tilde{23}^{q}(1+\{q,47\})} 89^{\tilde{11}^{q}(1+\{q,89\})} \cdots \tag{3.7.3}$$

Now because λ_p and p are always different and share no common factor, in the cases that λ_p equals q, then p itself cannot equal q. Thus we can cancel all valuation-braces:

$$2^q - 1 = 3^{\tilde{2}^{q}(1)} 7^{\tilde{3}^{q}(1)} 23^{\tilde{11}^{q}(1)} 31^{\tilde{5}^{q}(1)} 47^{\tilde{23}^{q}(1)} 89^{\tilde{11}^{q}(1)} \cdots \tag{3.7.4}$$

and we have a pretty direct representation for the primefactor-decomposition of mersenne-numbers M_q. Note, that in the example I've still documented the α_p-values being 1; because it is not yet known whether there exists another wieferich-prime (having $\alpha_p>1$) at all or even with a cyclelength which is prime (For the cyclotomic version of $f_b(n)$ with base $b=3$ there exists a "generalized Wieferich prime" $p=11$, which has a prime cyclelength $\lambda_p=5$ and occurs with $\alpha_{11}=\{3^{\lambda_{11}}-1,11\}=2$ so such a similar occurence for Mersenne-numbers cannot easily be excluded) .

Mersenne-primes

Now, when is a Mersenne-number also prime?

We see, that the cycle-length $\lambda_p=11$ occurs two times: at $p=23$ and at $p=89$, thus the mersenne-number $M_{11}=2^{11}-1$ has that two primefactors and is thus not prime. Consequently $M_{11}=2047$ does not occur in the list of possible primefactors of another M_m . The prime cycle-lengthes $\lambda_p=2,3,5,\ldots$ occur ***only once*** or: "for ***one primefactor p only***", so $q=2,3,5,\ldots$ define mersenne-numbers with only one primefactor and such M_q are now "mersenne-primes".

"Unique" or "unshared" primes (primal cycle-lengthes λ)

I tend to introduce that property as new term: the primal cycle-lengthes, which occur only once may be called themselves (Mersenne) "*unique primes*" and the other prime lengthes (which occur for more primefactors *p*) may be called (Mersenne) "*shared primes*". Then we can say: the set ***U*** *= [2,3,5,7,13,17,19,31,...]* of unique/unshared primes *u* defines the set of prime Mersenne-numbers M_u

(3.7.5) *Let* $2^u - 1 = M_u$ *then* $u \in \mathbf{U} \leftrightarrow M_u$ *is prime*

Do all prime cycle-lengthes occur?

If the above list is short, we'll miss the prime cycle-length $\lambda_p=7$. We could ask, whether all prime cycle-lengthes must occur.

The answer is easy: $M_q = 2^q-1$ is either prime or composite.

- If M_q is prime, then it is also the primefactor having cycle-length $\lambda_p=q$; and λ_p exists.
- If M_q is composite then it has two or more primefactors, all with the same cycle-length $\lambda_{p_1}=\lambda_{p_2}= q$ (q is prime having no smaller factors) thus also this λ_p exists.

Since q can be any prime, this holds for all q and this means all primes occur at least one time as cycle-length λ_p.

3.8 Iterated Mersenne-numbers (iterated 2^n-1 where n is any positive integer)

We can look at the primefactor composition of iterated Mersenne-numbers, like

(3.8.1) $n_1 = 2^n-1$ $n_2 = 2^{n_1}-1$ $n_3 = 2^{n_2}-1$ $n_4 = ...$

The algebraic formulae introduced here help to express this for the primefactors.

When we look at a primefactor q then in most cases we need also the informations for the smaller primefactors, for instance for λ_q or its primefactors. So to make a list we note first the (trivial) evaluation

(3.8.2) $$\{n_1,2\}: \{2^n-1,2\} = 0$$

meaning that for no n n_1 can be even, can be divisibly by 2.

Then the list of odd primefactors shows slightly varying behaviour:

(3.8.3)
$$\{n_1,3\}: \{2^n-1,3\} = \underset{2}{\overset{n}{\sim}}\left(1+\{n,3\}\right)$$
$$\{n_2,3\}: \{2^{2^n-1}-1,3\} = \underset{2}{\overset{2^n-1}{\sim}}\left(1+\{2^n-1,3\}\right) = 0$$

so no iterated $n_{k>1}$ contains the primefactor 3

(3.8.4)
$$\{n_1,5\}: \{2^n-1,5\} = \underset{4}{\overset{n}{\sim}}\left(1+\{n,5\}\right)$$
$$\{n_2,5\}: \{2^{2^n-1}-1,5\} = \underset{4}{\overset{2^n-1}{\sim}}\left(1+\{2^n-1,5\}\right) = 0$$

so no iterated $n_{k>1}$ contains the primefactor 5

$$\{n_1,7\}:\{2^n-1,7\} = \underset{3}{\overset{n}{\sim}}(1+\{n,7\})$$

(3.8.5)
$$\{n_2,7\}:\{2^{2^n-1}-1,7\} = \underset{3}{\overset{2^n-1}{\sim}}(1+\{2^n-1,7\}) = \underset{2}{\overset{n}{\sim}}\left(1+\underset{3}{\overset{n}{\sim}}(1+\{n,7\})\right)$$

$$\{n_3,7\}:\{2^{n_2}-1,7\} = \underset{3}{\overset{n_2}{\sim}}(1+\{2^{n_2}-1,7\}) = 0$$

so n_2 where n is even contain the primefactor 7, but no iterated $n_{k>2}$

$$\{n_1,11\}:\{2^n-1,11\} = \underset{10}{\overset{n}{\sim}}(1+\{n,11\})$$

(3.8.6)
$$\{n_2,11\}:\{2^{2^n-1}-1,11\} = \underset{10}{\overset{2^n-1}{\sim}}(1+\{2^n-1,11\}) = 0$$

so no iterated $n_{k>1}$ contains the primefactor 11

$$\{n_1,23\}:\{2^n-1,23\} = \underset{11}{\overset{n}{\sim}}(1+\{n,23\})$$

(3.8.7)
$$\{n_2,23\}:\{2^{2^n-1}-1,23\} = \underset{11}{\overset{2^n-1}{\sim}}(1+\{2^n-1,23\}) = \underset{10}{\overset{n}{\sim}}\left(1+\underset{11}{\overset{n}{\sim}}(1+\{n,23\})\right)$$

$$\{n_3,23\}:\{2^{n_2}-1,23\} = \underset{11}{\overset{n_2}{\sim}}(1+\{n_2,23\}) = 0$$

so n_2 where $[n:10]=1$ contain the primefactor 23, but no iterated $n_{k>2}$

Of special interest is by all this the primefactor $p=127$

$$\{n_1,127\}:\{2^n-1,127\} = \underset{7}{\overset{n}{\sim}}(1+\{n,127\})$$

(3.8.8)
$$\{n_2,127\}:\{2^{n_1}-1,127\} = \underset{7}{\overset{n_1}{\sim}}(1+\{n_1,127\}) = \underset{3}{\overset{n}{\sim}}\left(1+\underset{7}{\overset{n}{\sim}}(1+\{n,127\})\right)$$

$$\{n_3,127\}:\{2^{n_2}-1,127\} = \underset{7}{\overset{n_2}{\sim}}(1+\{n_2,127\}) = \underset{2}{\overset{n}{\sim}}\left(1+\underset{3}{\overset{n}{\sim}}\left(1+\underset{7}{\overset{n}{\sim}}(1+\{n,127\})\right)\right)$$

$$\{n_4,127\}:\{2^{n_3}-1,127\} = \underset{7}{\overset{n_3}{\sim}}(1+\{n_3,127\}) = 0$$

so even n_3 where $[n:2]=1$ contain the primefactor 127, but no iterated $n_{k>3}$

Sidenote: since we know that $M_{127} = 2^{127}-1$ is prime, we can easily copy that pattern to conclude, that first $\{n_5, M_{127}\}=0$

Wieferich primes:

(3.8.9)
$$\{n_1,1093\}:\{2^n-1,1093\} = \underset{364}{\overset{n}{\sim}}(2+\{n,1093\})$$

$$\{n_2,1093\}:\{2^{2^n-1}-1,1093\} = \underset{364}{\overset{2^n-1}{\sim}}(2+\{2^n-1,1093\}) = 0$$

while n_1 can contain 1093 to the second power (but not to the first!) no iterated $n_{k>1}$ contains the primefactor 1093

$$\{n_1,3511\}:\{2^n-1,3511\} = \underset{1755}{\overset{n}{\sim}}(2+\{n,3511\})$$

(3.8.10)
$$\{n_2,3511\}:\{2^{2^n-1}-1,3511\} = \underset{1755}{\overset{2^n-1}{\sim}}(2+\{2^n-1,3511\}) = \underset{36}{\overset{n}{\sim}}\left(2+\underset{1755}{\overset{n}{\sim}}(2+\{n,3511\})\right)$$

$$\{n_3,3511\}:\{2^{n_2}-1,3511\} = \underset{36}{\overset{n_1}{\sim}}(2+\{2^{n_2}-1,3511\}) = 0$$

while n_1 can contain 3511 to the second power (but not to the first!), n_2 can contain it to the $2^{nd},4^{th},5^{th},6^{th},\ldots$ (but not to the 1^{st} or 3^{rd}(!)) power), and no iterated $n_{k>2}$ contains the primefactor 3511

What we are essentially doing here is to iterate the lambda-function λ_p. This includes here also to generalize it to λ_m where m is no more prime. Iterations of this tend always to smaller numbers and finally to zero, so we can see, that for each primefactor p we have $\{n_k,p\}=0$ for some $k>K$ where the upper bound $K>1$ is some small number (equal or smaller than the *height* of the iterated base-2-logarithm $\log_2(1+x)$ applied to p).

3.9 Cyclotomic expressions/repunits/*q-analogues*

An interesting variation of the function $f_{b,a}(n)$ is the "cyclotomic" version

(3.9.1) $c_{b,a}(n) = \dfrac{f_{b,a}(n)}{f_{b,a}(1)} = \dfrac{b^n - a^n}{b-a} = b^{n-1} + b^{n-2}a + b^{n-3}a^2 + \ldots + b\,a^{n-2} + a^{n-1}$

For the introduction let's look at that simpler expression with $a=1$ first

(3.9.2) $c_b(n) = \dfrac{f_b(n)}{f_b(1)} = \dfrac{b^n - 1}{b-1} = b^{n-1} + b^{n-2} + b^{n-3} + \ldots + b + 1 = [n]_b$

The latter expressions are also called "repunits", because in the number-system with base b they are written as string with n ones: 111111111_b . Also they are known as *q*-analogues $[n]_b$

The primefactorization changes in the following way. In the factorization of $f_b(n)$ we find at all primefactors, which are also factors of $f_b(1) = b - 1$ and thus having the order/ cyclelength $\lambda_p=1$. Name this group of primefactors with the letter r, then the primefactor-decomposition looks like

(3.9.3) $$b^n - 1 = \prod_{\substack{p\in odd\ primes\\ \lambda_p>1}} p^{\overset{n}{\sim}_{\lambda_p}(\alpha_p+\{n,p\})} * \prod_{\substack{r\in odd\ primes\\ \lambda_r=1}} r^{\overset{n}{\sim}_{1}(\alpha_r+\{n,r\})}$$

Since

(3.9.4) $$b^1 - 1 = \prod_{\substack{p\in odd\ primes\\ \lambda_p>1}} p^{\overset{1}{\sim}_{\lambda_p}(\alpha_p+\{1,p\})} * \prod_{\substack{r\in odd\ primes\\ \lambda_r=1}} r^{\overset{1}{\sim}_{1}(\alpha_r+\{1,r\})} = \prod_{\substack{r\in odd\ primes\\ \lambda_r=1}} r^{\alpha_r+\{1,r\}} = \prod_{\substack{r\in odd\ primes\\ \lambda_r=1}} r^{\alpha_r}$$

the construction of the cyclotomic version means just to remove that last product-expression:

(3.9.5) $$\frac{b^n - 1}{b-1} = \prod_{\substack{p\in odd\ primes\\ \lambda>1}} p^{\overset{n}{\sim}_{\lambda_p}(\alpha_p+\{n,p\})} * \prod_{\substack{r\in odd\ primes\\ \lambda=1}} r^{\{n,r\}}$$

and the primefactors r occur exactly when r divides n or $[\,n{:}r\,] = 1$.

> Sidenote: the right-most productterm in that formula is similar to the product-formula for n:
>
> $$n = \prod_{r\in\ primes} r^{\{n,r\}}$$
>
> which is interestingly also true, when in calculus the $\lim_{b\to 1} [n]_b$ is invoked (a well known property of "*q-analogues*")

3.10 Primefactors in the Lucas-sequence

A view on the modular properties of the Lucas-sequence, in a usenet-discussion 2005:

*Am 03.12.2005 03:53 schrieb c***@c***.com:*

>>>>>>It is easily shown that the Lucas sequence
>>>>>> 1, 3, 4, 7, 11, 18, 29, 47,
>>>>>>contains no multiples of 5.
>>>>
>>>>Right. The mod5 sequence is 1, 3, 4, 2, 1, 3, at which point you have a
>>>>string of 2 repeating, so you know it's an endless loop and will never hit 0.
>>
>>>>>>Moreover, it contains no multiples of 8, 12, 13, 17, 21, 28, 33, 37,
>>>>>>53, 57, 61, 69, 73, 77, 87, 89, 92, 93, or 97.
>>>>>>
>>>>>>Right now I do not know how to decide, for given n, whether the Lucas
>>>>>>sequence contains multiples of n. Similarly I would like to decide
>>>>>>for given a, b, n, whether the generalized Fibonacci sequence (a, b,
>>>>>>a+b, a+2b, 2a+3b, ...) contains multiples of n.
>
>>>>You could run through the sequence mod n until it repeats. It will
>>>>definitely repeat before term n^2. (Maybe somebody else can put a tighter
>>>>bound on it.)
>>
>> The following link:
>>
>> http://www.mathpages.com/home/kmath078.htm
>>
>> has some relevant calculations; in particular, for the Lucas sequence,
>> the upper bound appears to be 4*n, while for the Fib. sequence, it is
>> 6*n.
>>

My answer, which I also formatted/edited a bit for this article:

Hi -

since you coin the cyclicity of the modules, I'll apply my approach to that question: to find the "order of the cyclic subgroup modulo any prime p" (call it $\lambda_p(b,a)$) and analyze them in a joint framework for all primefactors; here for the expression

$$g_{b,a}(n) = b^n + a^n \qquad (3.10.1)$$

where

$$b= (1+\sqrt{5})/2 = \varphi \qquad a=(1-\sqrt{5})/2 = -1/\varphi \qquad (3.10.2)$$

which generates the Lucas-sequence $<2,1,3,4,7,\ldots>$ for subsequent $n>=0$.

The pair of bases (b,a) has irrational values, so some "nonreglar" effects concerning cycle-lengthes etc. may occur. For instance for prime $p=7$ the cycle-length λ_p is

$$\lambda_7(\varphi,-1/\varphi) = 8$$

and the first occurence of the primefactor $p=7$ in $g(n)$ is at $n=4$. Thus, instead of having a cycle-length being a divisor of $p-1$ we find a cycle-length being a divisor of $p+1$.

Translation to the fibonacci-sequence

To understand the following expression for primefactorization it may be useful to notice another identity.

According to the discussion (*here in chap 1*) we can see $g_{b,a}(n)$ as quotient $f_{b,a}(2n)/f_{b,a}(n)$, and the function $f_{b,a}(n)/f_{b,a}(1)$ is known as the generating function for the sequence of fibonacci-numbers $< 0,1,1,2,3,5,8,13,21,\ldots>$ for $n \geq 0$.

So we can write

$$(3.10.3)\quad g_{b,a}(n) = \frac{f_{b,a}(2n)/f_{b,a}(1)}{f_{b,a}(n)/f_{b,a}(1)} = \frac{(b^{2n}-a^{2n})/(b-a)}{(b^n-a^n)/(b-a)} = \frac{b^{2n}-a^{2n}}{b^n-a^n}$$

The cycle-lengthes λ_p and the exponent at first occurrence α_p must be determined for each prime individually; with that heuristics we get the following primefactor-decomposition for $f_{b,a}(n)/f_{b,a}(1) = (b^n-a^n)/(b-a)$:

$$(3.10.4)\quad \frac{b^n-a^n}{b-a} = 2^{\tilde{3}^n\left(1+\{n,2\}+\tilde{2}^n(1)\right)}3^{\tilde{4}^n\{3n,3\}}5^{\tilde{5}^n\{n,5\}}7^{\tilde{8}^n\{7n,7\}}11^{\tilde{10}^n\{11n,11\}}13^{\tilde{7}^n\{13n,13\}}17^{\tilde{9}^n\{17n,17\}}\cdots$$

where I used the shorter notation $\{p\cdot n\ ,\ p\}$ for $(1+\{n,p\})$.

It is interesting, that at $p=2,3,7,13,17,\ldots=5k\pm2$ we have the cycle-lengthes related to $p+1$, and at $p=11,\ldots,\ldots=5k\pm1$ related to $p-1$, and at $p=5$ even directly related to p itself. (We have seen the latter effect in the paragraph about the cyclotomic functions). Heuristically it seems that

$$(3.10.5)\quad \begin{array}{ll} \text{cycle-length equals } p(=5) & : \text{for } p=5 \\ \text{cycle-length divisor of } p-1 & : \text{for } p\equiv\pm1 \pmod 5 \\ \text{cycle-length divisor of } p+1 & : \text{for } p\equiv\pm2 \pmod 5 \end{array}$$

So, if there is no "wieferich" effect and thus all "initial exponents" α equal 1, then the above formula could even more be simplified.

Now, $g_{b,a}(n)$ can be computed by $f_{b,a}(2n)/f_{b,a}(n)$, and its primefactor-decomposition begins as follows:

$$(3.10.6)\quad b^n+a^n = \frac{2^{\tilde{3}^{2n}\left(\tilde{2}^{2n}+\{4n,2\}\right)}3^{\tilde{4}^{2n}\{6n,3\}}5^{\tilde{5}^{2n}\{2n,5\}}7^{\tilde{8}^{2n}\{14n,7\}}11^{\tilde{10}^{2n}\{22n,11\}}13^{\tilde{7}^{2n}\{26n,13\}}17^{\tilde{9}^{2n}\{34n,17\}}\cdots}{2^{\tilde{3}^{n}\left(\tilde{2}^{n}+\{2n,2\}\right)}3^{\tilde{4}^{n}\{3n,3\}}5^{\tilde{5}^{n}\{n,5\}}7^{\tilde{8}^{n}\{7n,7\}}11^{\tilde{10}^{n}\{11n,11\}}13^{\tilde{7}^{n}\{13n,13\}}17^{\tilde{9}^{n}\{17n,17\}}\cdots}$$

Like in the earlier chapter we collect exponents; because the valuations wrt $2n$ and n are equal except for the primefactor 2:

$$(3.10.7)\quad b^n+a^n = 2^{\tilde{3}^{2n}\left(\tilde{2}^{2n}+\{4n,2\}\right)-\tilde{3}^{n}\left(\tilde{2}^{n}+\{2n,2\}\right)}3^{(\tilde{4}^{2n}-\tilde{4}^{n})\{3n,3\}}5^{(\tilde{5}^{2n}-\tilde{5}^{n})\{n,5\}}7^{(\tilde{8}^{2n}-\tilde{8}^{n})\{7n,7\}}11^{(\tilde{10}^{2n}-\tilde{10}^{n})\{11n,11\}}$$
$$*13^{(\tilde{7}^{2n}-\tilde{7}^{n})\{13n,13\}}17^{(\tilde{9}^{2n}-\tilde{9}^{n})\{17n,17\}}\cdots$$

As in the example before, all primefactors with odd $\lambda()$ vanish because their "divides"-expression in the exponents cancel, so we have finally

$$(3.10.8)\quad b^n+a^n = 2^{\tilde{3}^{n}(2-\tilde{2}^{n})}3^{(\tilde{2}^{n}-\tilde{4}^{n})\{3n,3\}}7^{(\tilde{4}^{n}-\tilde{8}^{n})\{7n,7\}}11^{(\tilde{5}^{n}-\tilde{10}^{n})\{11n,11\}}\cdots$$

where the exponent of $p=2$ was also simplified.

From this we get the cycles for the primefactors $2<=p<=17$:

$p=2$: for $n=6k$ we have 2^1; for $n=6k-3$ we have 2^2
$p=3$: cycle-length 4, beginning at $n=2$
$p=5$: -does not occur -
$p=7$:cycle-length 8, beginning at $n=4$
$p=11$: cycle-length 10, beginning at $n=5$
$p=13$: -does not occur-
$p=17$: -does not occur-
…

and also we can conclude from the properties of the prime-factors in the fibonacci-sequence to that of the lucas-sequence. The (super-)cycles for higher exponents are powers of the according prime as indicated by their valuation-terms *{p*n , p}*.

3.11 A view into FLT

"Fermats last theorem"[6] () is somehow "the classical" problem to be expressed and studied with the "cyclic subgroups"-concept. We have the exponential diophantine equation

(3.11.1) $(f_{b,a}(n) =) \; b^n - a^n = c^n$

which is now known to have no solution given $b>a>c>0 \; , \; n>2$. This can -without loss of generality- be reduced to

(3.11.2) $b^q - a^q = c^q$

having *gcd(b,a)=1*, *q prime*. Because exactly one of *b,a,c* must be even and we can order them such that the rhs is odd, we can omit the primefactor *2* in the primefactordecomposition of the lhs as well.

Amateurish approaches (like early fiddlings of mine) to that problem can at most give likelihoods, and also the notation in the current framework does not evolve to an elementary solution of the problem. But it exposes another spotlight which I feel is intriguing: it reduces to the problem of existence of generalized wieferich-primes (with additional properties required).

We restate the primefactorization for the lhs $f_{b,a}(q)$ and exhibit conditions: *when can this primefactorization be a perfect power c^q where all primefactors of c have the same exponent q (or multiples of it)* ? Using the primefactorization of the lhs we get:

(3.11.3) $$b^q - a^q = \prod_{\substack{p \in odd \\ primes}} p^{\tilde{\lambda}_p^{\,q}(\alpha_p + \{q,p\})} \quad \overset{??}{=} \quad c^q$$

Here we know already, that the lhs, und thus the rhs, contains the factor *(b-a)* which defines a set of primes *r* having cycle-lengthes $\lambda_r = 1$, which we make explicite:

(3.11.4) $$b^q - a^q = \prod_{\substack{r \in odd \\ primes \\ \lambda = 1}} r^{\tilde{1}^{\,q}(\alpha_r + \{q,r\})} \prod_{\substack{p \in odd \\ primes \\ \lambda > 1}} p^{\tilde{\lambda}_p^{\,q}(\alpha_p + \{q,p\})}$$

We can sharpen this formula a bit more.

First, for the primes *p* we can remove the valuation-brace because for some *p* if the $\lambda_p > 1$ then it must $\lambda_p = q$. But it cannot occur, that at the same time λ_p and *p* are equal to a prime *q*. So we can reduce the second product-terms:

(3.11.5) $$b^q - a^q = \prod_{\substack{r \in odd \\ primes \\ \lambda = 1}} r^{\tilde{1}^{\,q}(\alpha_r + \{q,r\})} \prod_{\substack{p \in odd \\ primes \\ \lambda > 1}} p^{\tilde{\lambda}_p^{\,q}(\alpha_p)}$$

[6] "*last*" means here: "*last unsolved*", now correctly "Wiles' theorem"

Second, looking at the *r*-primefactors we see, that the valuation-brace as well can be removed when *r≠q*. So the primefactor *q* plays a special role if it is factor of *(b-a)* (means also: has cycle-length *1)*. So we make this explicite, too. The final formula looks then like

(3.11.6) $$b^q - a^q = q^{\overset{q}{\sim}_{\lambda_q}(\alpha_q+1)} \prod_{\substack{r\neq q\in odd\ primes\\ \lambda=1}} r^{\alpha_r} \prod_{\substack{p\neq q\in odd\ primes\\ \lambda=q}} p^{\alpha_p}$$

and separated for the two cases for *[b-a : q]=1* (or $\lambda_q=1$):

(3.11.7) *case 1: q is primefactor of (b–a) =$f_{b,a}(1)$; that means: $\lambda_q=1$ and $\{b-a,q\}=\alpha_q$*

$$b^q - a^q = q^{\alpha_q+\{q,q\}} \frac{b-a}{q^{\alpha_q+\{q,q\}}} \prod_{\substack{p\in odd\ primes\neq q\\ \lambda=q}} p^{\alpha_p}$$

$$= q^{\alpha_q+1} \prod_{\substack{r\in odd\ primes\\ \lambda=1, r\neq q}} r^{\alpha_r} \prod_{\substack{p\in odd\ primes\\ \lambda=q}} p^{\alpha_p}$$

(3.11.8) *case 2. q is not primefactor of (b-a); $\lambda_q<>1$ (and can thus not occur in c^q)*

$$b^q - a^q = (b-a) \prod_{\substack{p\in odd\ primes\\ \lambda=q}} p^{\alpha_p}$$

$$= \prod_{\substack{r\in odd\ primes\\ \lambda=1, r\neq q}} r^{\alpha_r} \prod_{\substack{p\in odd\ primes\\ \lambda=q}} p^{\alpha_p}$$

The set of primes *r* constitute the primefactors of *(b-a)* (excluding *q*), and this set is disjunct to the set of primes *p* which are furtherly multiplied to *(b-a)* to form the final value $f_{b,a}(q)$. So it is required, that the exponents α_r resp α_p of all this primefactors are equal to *q* or to a multiple of *q* . If also *q* is factor of *(b-a)* it must thus have exponent *q-1*. It is possible to construct infinitely many such *(b-a)*, which then means simply a perfect power, say $b-a=D^q$ or $b-a=q^{q-1}D^q$, thus $b=a+D^q$ or $b=a+q^{q-1}D^q$ with some (though not completely) arbitrary *a* and *D*.

But the problem occurs still with the set of primefactors *p*, (which necessarily is present since $b^q-a^q>(b-a)$), because ***all*** involved primefactors ***must be of the generalized wieferich type*** of order *q* (it must always be $\alpha_p(b,a)=q$); and while wieferich types with $\alpha_p(a,b)=2$ are already rare, that with $\alpha_p(a,b)=q>2$ are even more rare.

> *What means "rare"? In "Fermatquotients[7]" I studied the construction of (b-a) such that for a given prime p and a nontrivial pair (b,a) the value $\alpha_p(b,a)$ is arbitrarily greater than 1. The term "rare" means according to that text roughly, that in a set of n solutions (b,a) with fixed a and consecutively increasing b providing $\alpha_p(b,a)=2$, the number n_q of solutions for $\alpha_p(b,a)=q$ is of order $n^{1/q}$*

[7] online: http://go.helms-net.de/math/expdioph/fermatquotients.pdf