Fermat-/Euler-quotients

$(b^{p-1} - 1)/p^k$ with arbitrary k

Abstract: Fermat quotients with arbitrary k (=α, see below) are considered on an introductory level.

While the ongoing research on fermat-quotients is concerned with the very difficult problem to find an appropriate primenumber p for α>1 and a given base b, the article here is primarily concerned with the much simpler problem of finding appropriate bases b if the primenumber p is given.

In chapter 3 I do a first step into the more difficult problem of finding primes for given small bases. I begin generalizing the problem to composite n instead of prime p, making it an "Euler-quotient" to get more heuristical data for analysis. Some nice structural insight appears.

Gottfried Helms *20.03.2017* *version 2.3.6 (textcorrections)*

Contents:

1. Intro and definitions

Here I present a method how to find bases *b* in the so-called "***Fermat-quotient***"

$$f_p(b) = (b^{p-1} - 1)/p^k \qquad \text{being integer for certain } k>0$$

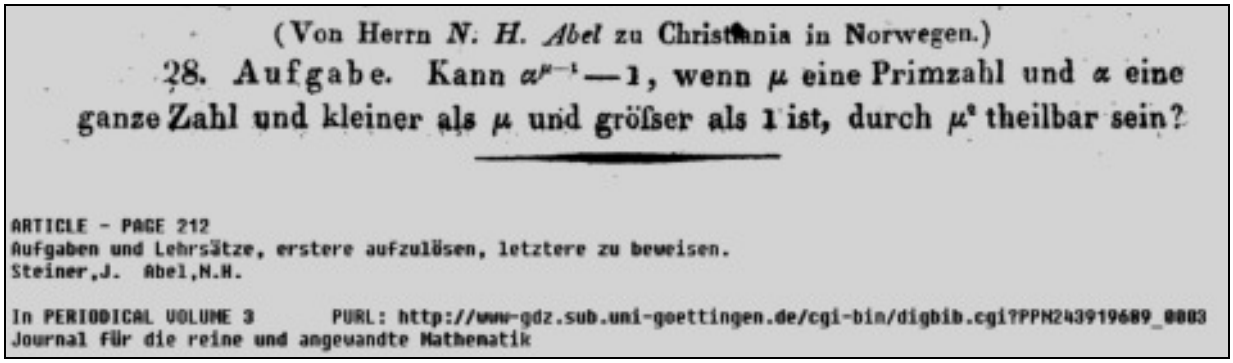
or, differently written,

$$b^{p-1} \equiv 1 \pmod{p^k} \qquad // \text{ for } k>0$$

for a given, arbitrary (high) *k>0* (as discussed – for instance – in [1],[3]) .

If this congruence holds for a certain pair *(b,p)* with *k>0*, then I'll write that we have a "*fq of k'th degree*", and if *k>1* I'll write "*of high degree*". Here we are concerned with cases where *k>1*.

A historical reference is due to Niels Abel:


(Von Herrn *N. H. Abel* zu Christiania in Norwegen.)

28. Aufgabe. Kann $\alpha^{\mu-1}-1$, wenn μ eine Primzahl und α eine ganze Zahl und kleiner als μ und gröfser als 1 ist, durch μ^2 theilbar sein?

ARTICLE - PAGE 212
Aufgaben und Lehrsätze, erstere aufzulösen, letztere zu beweisen.
Steiner,J. Abel,N.H.

In PERIODICAL VOLUME 3 PURL: http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN243919689_0003
Journal für die reine und angewandte Mathematik

This problem is also related to the "Wieferich-primes" , which occur as special case of *p* using *b=2, k=2* .

There are not many known pairs *(b,p)*, especially with small *b*. To get a broader view into the structure of the problem I'll also generalize it to that of composite *n* instead of prime *p* in

$$f_n(b) = (b^{\varphi(n)} - 1)/n^k$$

or written in (mod)-notation in

$$b^{\varphi(n)} \equiv 1 \pmod{n^k} \qquad // \text{ for } k>1$$

which is then connected with the Euler *totient-function.* With L. Skula (*see [Skula]*) I call this "*generalized Fermat-quotient*" or simply "*Euler-quotient*".

I discuss two views of things here. The first part is to discuss how to find appropriate bases *b* when a fixed *p* is given, and even a certain high *k* is asked for. This is a relatively easy matter, but which I didn't find worked out in easily available online articles – so I'll enclose my fiddling with this here.

This may also be a good eye-opener for the more difficult problem to find an appropriate *p* (or *n*) when a base *b* is given, especially if *b* is small. At least I find some structure for the case of the Euler-quotient case which I've not come across in the articles available to me so far.

All is done on the level of a hobby mathematician/number theorist, so don't expect really new or advanced results in this compilation.

Before the mathematical considerations in chap *2* and *3*, I'll introduce some useful definitions/notations.

1.1. Two operator-notations

Define the notation ***[n:p]*** as

(1.1) $[n: p] := 1$ if p divides n,
$[n: p] := 0$ if p does not divide n

Define the notation ***{n,p}*** as

(1.2) $\{n, p\} := \Sigma_{k=1..oo} [n: p^k]$ the exponent of the power to which p is a factor of n

Example:

$\{x \cdot p^m, p\} = m$ // gcd(x,p)=1

Then the above problem can be written as

(1.3) find pairs of b,p such that
$\{b^{p-1} - 1, p\} = k$ for arbitrary $k > 1$

Note, that the exponent at b need not always be $p-1$ but may also be smaller; more precisely a divisor of $p-1$, according to a "length-function" λ (lambda) .

1.2. The "length"-function λ

This length-function λ is also the "*order of the multiplicative cyclic subgroup mod p*" and may be described by an implicite definition:

(1.4) $\lambda_{b,1}(p) := k$ where $b^k - 1 \equiv 0 \pmod p$ and $k>0$ is minimal

Differently said: $\lambda > 0$ is the smallest exponent k when p occurs as factor of $b^k - 1$. Note, that λ is a divisor of $p-1$, and that the expression *(1.3)* is compatible with Fermat's little theorem and Euler's extension. A consequence is that

(1.5) $b^{\lambda} - 1 \equiv 0 \pmod p$ // by definition (1.4)
$b^{\lambda p^k} - 1 \equiv 0 \pmod{p^{k+1}}$ // by Euler's extension of Fermat's little theorem

Using the above operator-notation:

$\{b^{\lambda} - 1 , p\} \geq 1$
or $\{b^{\lambda p^k} - 1, p^{k+1}\} \geq 1$
or $\{b^{\lambda p^k} - 1, p\} \geq 1+k$

The value of this length-function has no known simple relation to p and b and must be found empirically. (see Appendix 3.3) Also I use the simple letter λ without parameters if they are obvious from context, although each pair of base b and prime p defines its own value for λ !

1.3. The "initial power"-function α

Because at λ (precisely written: $\lambda_{b,1}(p)$) the value $b^{\lambda} - 1 = x \cdot p^k$ may contain p to a power $k>1$, it is useful to refer to this exponent by a function-name as well. This introduces the α-*("alpha")*–function by the implicite definition:

(1.6) $\alpha_{b,1}(p) := \{b^{\lambda} - 1, p\} = \alpha$

Thus, α is the exponent of p as factor in

$$b^{\lambda} - 1 \equiv 0 \ (mod\ p^{\alpha}\ )$$

or – the power of p's first occurrence when the exponent at b grows from 1.

Similarly to the λ–function I'll omit the parameters b and p at α if they are obvious from context; so instead of $\alpha_{b,1}(p)$ I simply write α in most cases

The value for α must also be found by direct search.

Sidenote: Fermat's little theorem gives $k+1$ in the exponent of p in (1.5) only as a lower bound; the supplement by the α–function however allows to have a precise expression for that exponent. We have

(1.7) $$b^{(p-1)p^k} - 1 \equiv 0 \ \ (mod\ p^{k+1})$$

by Euler/Fermat, where $k+1$ is a lower bound. Using the α–function we can say

(1.8) $$b^{\lambda p^k} - 1 \equiv 0 \ \ (mod\ p^{k+\alpha})$$

which is an improvement, since $k+\alpha$ is the actual power of p, which is often of more interest. Furthermore we can state the exact relation in the currently proposed notation:

(1.9) $$\{ b^{\lambda p^k} - 1 \ , \ p \ \} = \alpha + k \qquad // \text{Proof: see Appendix 3}$$

1.4. Remarks on the cyclicityness

Varying exponent: From the Fermat/Euler-theorem it is known, that the occurence of exponent k in p^k with fixed base but varing exponent n in the expression $b^n - 1 = x \cdot p^k$ is cyclic, and has supercycles if we refer to k'th powers of p. According to the Fermat/Eulertheorem for primefactors p for some m,c and x:

$$b^{\ m \cdot (p-1)} - 1 = x \cdot p$$
$$b^{\ m \cdot (p-1) \cdot p^c} - 1 = x \cdot p^{1+c}$$

where x may contain some more powers of p.

One can refine then for primes $p<>2$ and varying n using the newly introduced notation:

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

Consider the sequence of natural numbers: then the powers of p are just the same as in the sequence of natural numbers when written as

$$\{b^{(p-1) \cdot n} - 1, \ p\} = \alpha + \{n,p\}$$

and if we call a "cycle" the occurrence of p in n and a "supercycle" (of order k) for the occurrence of p^k in n , then all cycles and supercycles have a "natural" origin at α which is in most cases 1. Why can we call this "origin"? Because this is the unique number, where all cycles and supercycles meet one time.

Varying base: This is different in the current discussion, where the exponent is fixed and the base is varying. As I show in chap 2, we have the same type of cyclicity, but all cycles and supercycles have "a different origin" – or we must say, they don't have an origin at all, because the offsets of their first occurrences (when n grows from 1) are not matching at a common index and are non-predictably related to all residues $mod\ p$.

1.5. Some illustrative results for p^{α} divides $b^{p-1} - 1$ with high α

Notes:

- here I use $b^{\lambda} - 1$ instead of $b^{p-1} - 1$, (however sometimes $\lambda=p-1$)
- I use the notation $b^{\lambda} - 1 = x \cdot p^{\alpha}$; *where* $gcd(x,p)=1$ instead of the usual ($mod\ p^k$)-notation here, because it is an exact equation for α

(1.10) $324^3 - 1 = x \cdot 7^3$ or $\{324^3 - 1 , 7 \} = 3$

(1.11) $740862^6 - 1 = x \cdot 7^7$ or $\{740862^6 - 1 , 7\} = 7$

(1.12) $175909088838^{12} - 1^{12} = x \cdot 13^{12}$

(1.13) $5716340889977719^{11} - 1^{11} = x \cdot 23^{11}$

(1.14)
$$b = 42248895967042508283279206813235258854234225251519346683626565404363754705104377419988318310806044652742101150754590906889 \\ 11708304105979739854099818497271594989072901907337041444704404036891977239754652500794951539355221519064613575802650426875 \\ 6338497009455353525052$$
$b^{113} - 1 = x \cdot 227^{113}$

(1.15)
$$b = 30846926358565474366588815022736512012844002055947545237497248 \\ 09339582975913647747172718009227981703286336472733735786868766 \\ 41116333308635579981499259406250338670447097474137235785030122 \\ 83030188977619301207729256928448642627167427911233911577463783 \\ 80803894164426401736021854771492609728365807713161035598381642 \\ 15684923136020602990366513935980832357136685938502067398097013 \\ 81127730382719677386436581349052903589192579125441471992399808 \\ 31307834930083704970998074730259152868571529771291132868518975 \\ 85742890021876438425099209080636582633848590695561950529153764 \\ 37210705068090972302143710459484981269701445163553608379816$$
$b^{256} - 1 = x \cdot 257^{256}$

2. Observations on cycles and high exponents of p

2.1. Initial observations

If we approach

$$f_{p,\alpha}(b) = (b^{\lambda} - 1)/p^{\alpha} \qquad \text{being integer for } \alpha>0$$

or $\alpha = \alpha_{b,1}(p) = \{b^{p-1} - 1,\ p\}$

for a given p and α heuristically, then we can observe,

that the occurences of $\alpha_{b,1}(p)$ follow a cyclic scheme,

and also that these cycles are overlaid by supercycles up to arbitrary height providing arbitrary high α and

where the cycles-lengthes agree to the related powers of p.

Here is a small part of a longer table (see Appendix 1), which lists α and λ for the primes $2,3,5,7,11,13,17$ for some small bases b. The entries are "α_λ" where, if $\alpha=1$ it is omitted and only "λ" is documented. So we see, for instance in the column of prime $p=11$ and row for $3^n - 1$ the entry "2_5", which means $3^5 - 1 \equiv 0 \pmod{11^2}$

	2	3	5	7	11	13	17
1^n-1:	1	1	1	1	1	1	1
2^n-1:	.	2	4	3	10	12	8
3^n-1:	1	.	4	6	2_5	3	16
4^n-1:	.	1	2	3	5	6	4
5^n-1:	1	2	.	6	5	4	16
6^n-1:	.	.	1	2	10	12	16
7^n-1:	1	1	2_4	.	10	12	16
8^n-1:	.	2_2	4	1	10	4	8
9^n-1:	1	.	2	3	2_5	3	8
10^n-1:	.	2_1	.	6	2	6	16
11^n-1:	1	2	1	3	.	12	16
12^n-1:	.	.	4	6	1	2	16
13^n-1:	1	1	4	2	10	.	4
14^n-1:	.	2	2	.	5	1	16
15^n-1:	1	.	.	1	5	12	8
16^n-1:	.	1	1	3	5	3	2
17^n-1:	1	2_2	4	6	10	6	.
18^n-1:	.	.	2_4	3_3	10	4	1
19^n-1:	1	2_1	2	3_6	10	2_12	8

Don't mind the coloring-scheme here, I'll discuss this in the appendix.

What the table exhibits by eyeball inspection is cyclicitiness of the lengthes λ for a fixed p over increasing bases b (with cycle-length p) and also of the α -values with cycle-lengthes of powers of p.

Indeed, both can easily be verified by representation of base b in terms of a polynomial in p (or "*p-adic*"-representation of b)

(2.1) $$b = d_0 + d_1\, p + d_2\, p^2 + \ldots + d_k\, p^k$$

where the d_k are *digits* $0 \le d_k < p$ and by the analysis of the binomial-expansion of its powers.

As a consequence, this cycling allows to compute nontrivial bases b which provide fermat-quotients with arbitrary high powers of p.

2.2. Initial example computation

Due to the cyclicity this requires simply to express the base b in the digit-system to base p and to apply a small generation-rule. Below is an example for $p=7$. We begin with the residue $d_0 = 3$, use this as first base b_0 and apply the λ -information $\lambda_{3,1}(7)=6$ to form

$$b_0^{\lambda_{3,1}(7)} - 1 \equiv 3^6 - 1 \equiv 0 \pmod{7^1}$$
$$\text{or:} \quad \{ b_0^{\lambda_{3,1}(7)} - 1 \, , \, 7 \} = 1$$

Then by a simple heuristic we find the subsequent b_k providing fermat-quotients with higher powers of p:

k(=α)	$b^{p-1} - 1$	$\equiv 0 \bmod(p^{\alpha})$	"b" in digitsystem base p
1	$3^6 - 1$	$\equiv 0 \bmod(7^1)$	$3_{\text{base } 7}$
2	$31^6 - 1$	$\equiv 0 \bmod(7^2)$	$4\ 3_{\text{base } 7}$
3	$325^6 - 1$	$\equiv 0 \bmod(7^3)$	$6\ 4\ 3_{\text{base } 7}$
4	$1354^6 - 1$	$\equiv 0 \bmod(7^4)$	$3\ 6\ 4\ 3_{\text{base } 7}$
5	$1354^6 - 1$	$\equiv 0 \bmod(7^5)$	$0\ 3\ 6\ 4\ 3_{\text{base } 7}$
6	$34968^6 - 1$	$\equiv 0 \bmod(7^6)$	$2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
7	$740862^6 - 1$	$\equiv 0 \bmod(7^7)$	$6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
8	$2387948^6 - 1$	$\equiv 0 \bmod(7^8)$	$2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
9	$25447152^6 - 1$	$\equiv 0 \bmod(7^9)$	$4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
10	$146507973^6 - 1$	$\equiv 0 \bmod(7^{10})$	$3\ 4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
11	$1276408969^6 - 1$	$\equiv 0 \bmod(7^{11})$	$4\ 3\ 4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
12	$9185715941^6 - 1$	$\equiv 0 \bmod(7^{12})$	$4\ 4\ 3\ 4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
13	$78392151946^6 - 1$	$\equiv 0 \bmod(7^{13})$	$5\ 4\ 4\ 3\ 4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
14	$272170172760^6 - 1$	$\equiv 0 \bmod(7^{14})$	$2\ 5\ 4\ 4\ 3\ 4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
15	$950393245609^6 - 1$	$\equiv 0 \bmod(7^{15})$	$1\ 2\ 5\ 4\ 4\ 3\ 4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
16	$10445516265495^6 - 1$	$\equiv 0 \bmod(7^{16})$	$2\ 1\ 2\ 5\ 4\ 4\ 3\ 4\ 2\ 6\ 2\ 0\ 3\ 6\ 4\ 3_{\text{base } 7}$
…	…	…	…

Note, that due to the composition beginning at $d_0 <> 0$ the b_k are automatically co-prime to p and can have any further characteristic, especially can itself be prime.

The yellow marker indicates, that at $k=4$ the α-function does a jump: the value jumps from $\alpha = 3$ at $k = 4$ to $\alpha = 5$ at $k = 5$ because the next digit d_4 is zero. There are also cases, where these jumps are bigger; I observed cases of two and even three consecutive zero-digits, and it would be interesting to discover the conditions of such occurences and of jumps of higher degree.

2.3. Second example computation

Another example: of direct computation of the number b using the moduli and base-p-representation and a modulus/digit-translation-table:

> Start with a residue $(mod\ p)$, say 3, set this as base b_0. Get the length-info $\lambda_{b,1}(p)$, which is 6 here. So $3^6 \equiv 1\ (mod\ 7)$. Express $y=3^6$ in digits of numbersystem base 7: ="2061"$_7$. The last digit is 1, so indeed the residue condition is $y_0 \equiv 1\ (mod\ 7^1)$.
>
> To get the next number b_1, which gives then $b_1^6 = y_1 \equiv 1\ (mod\ 7^2)$, the second digit in y_0 (which is 6 here) must become zero in y_1, so we must have y_1="$???01$"$_{base\ 7}$. This can be achieved, if we add $4 \cdot 7$ to b_0 (or simply prefix b with the digit 4):
>
> $$b_1 = 4 \cdot 7^1 + b_0 = 31 .$$
>
> We verify, that $y_1 = 31^6 \equiv 1\ (mod\ 7^2)$ and repeat the process ad libitum to get consecutive b_k up to any finite k satisfying $b_k \equiv 1\ (mod\ 7^k)$.

```
                                                        1|" ->3
"3"^6  =                                          "2 0 6|1 " ->4
"4 3"^6   =                          "3 0 6 6 4 4 4 1 2|0 1 " ->6
"6 4 3"^6   =      "5 0 3 1 3 4 0 2 2 1 5 6 3 0 1|0 0 1 " ->3
"3 6 4 3"^6 ="...3 6 5 2 3 1 3 2 0 2 6 5 4 3 0|0 0 0 1 " ->0
          "... 1 3 6 5 2 3 1 3 2 0 2 6 5 4 3|0 0 0 0 1 " ->2
          "... 2 4 5 0 2 5 2 3 5 1 3 1 3 2|0 0 0 0 0 1 " ->6
          "... 4 1 0 5 2 0 2 4 0 2 1 1 3|0 0 0 0 0 0 1 " ->2
          "... 2 4 2 2 3 5 4 0 0 3 5 6|0 0 0 0 0 0 0 1 " ->4
          "... 2 0 0 0 4 1 3 0 3 6 1|0 0 0 0 0 0 0 0 1 " ->3
          "... 2 3 4 4 2 5 6 6 3 6|0 0 0 0 0 0 0 0 0 1 " ->4
          "... 6 2 5 0 1 6 3 1 6|0 0 0 0 0 0 0 0 0 0 1 " ->4
          "... 5 3 0 6 2 2 5 4|0 0 0 0 0 0 0 0 0 0 0 1 " ->5
          "... 2 3 1 3 3 0 3|0 0 0 0 0 0 0 0 0 0 0 0 1 " ->2
          "... 3 6 1 5 0 5|0 0 0 0 0 0 0 0 0 0 0 0 0 1 " ->1
 ...    ...
```

Translation table

observe digit
-> use digit for new base "b"

0	->0
1	->3
2	->6
3	->2
4	->5
5	->1
6	->4

Moreover: there is a simple rule for the translation of the critical digit in y_k into the prefix for the next b_{k+1}: it seems to be just $k \cdot b_0\ (mod\ p)$. See the translation table above (but I didn't crosscheck this for other initial residue-classes or other bases yet).

The sequence of b_k can be generated by

$$b_0 = (\text{any nonzero residue of } n\ (mod\ p)\ )$$
$$b_{k+1} = d_{k+1} \cdot p^{k+1} + b_k$$

where the sequence of digits d_k is apparently aperiodic and I assume that it must be determined empirically.

(In my Pari/GP-code I did not yet use this translation table but the simple search for the appropriate next digit by trying the digits from 0 to $p-1$)

Later remark: the bases can easily be found using standard functions in Pari/GP and its "*p-adic*" data-type:

```
p = 7          \\ set some example primefactor
b0 = 2         \\ set some example initial base
lambda = znorder(Mod(b0,p))  \\ =3; the value of the lambda/"length" function

a = b0 + O(p^5) \\ displays b0 in the p-adic representation up to p^4
teichmuller (a) \\ displays the digits d0,d1,d2,d3,d4 by p-adic representation

k=4  \\ try some example, such that alpha = k = 4
bk = lift (teichmuller( b0+ O(p^k))) \\ gives the base bk in numerical format
                                     \\ which allows {bk^lambda - 1, p} = k = 4
```

2.4. The final formula for computation of the subsequent b_k

The digits d_k and thus the values of b_k can be determined without search by a simple recursive formula.

The key idea is, that, if we have the identity with a certain k,

(2.4.1) $$\{b_{k-1}^m - 1, p\} = k \qquad gcd(b,p)=1$$

it follows that, with a certain digit d_k

(2.4.2) $$\{(b_{k-1}+d_k \cdot p^k)^m - 1, p\} = k+1$$

This can uniquely be solved using the binomial-expansion of the parenthese. And the initial condition *(2.4.1)* for $k=1$ can be solved using Fermat's little theorem .

Proof:

Given a fixed prime p, we select b_0 $(1<b_0<p)$ and have to compute $\lambda = \lambda_{b_0,1}(p)$, so we have the triple $[p,b_0, \lambda]$ as initialization of the recursion for $k=0$. Now we expand (2.4.2) and evaluate the binomial-coefficients assuming that

$$b_k = b_{k-1} + d_k p^k$$

such that

$$b_k^m - 1 = (b_{k-1}+d_k p^k)^m - 1 = x_k p^{k+1}$$

(2.4.2) $$(b_{k-1}+d_k p^k)^m - 1 = x_k p^{k+1}$$
$$b_{k-1}^m + m\, b_{k-1}^{m-1} d_k p^k + (m:2)\, b_{k-1}^{m-2} (d_k p^k)^2 + \dots + (d_k p^k)^{m-1} - 1 = x_k p^{k+1}$$

Here we can put the -1 to b_{k-1}^m and we know, that this is $x_{k-1}p^k$:

$$x_{k-1}p^k + m\, b_{k-1}^{m-1} d_k p^k + (m:2)\, b_{k-1}^{m-2} (d_k p^k)^2 \dots + (d_k p^k)^{m-1} = x_k p^{k+1}$$

We divide this by the common factor p^k getting

$$x_{k-1} + m\, b_{k-1}^{m-1} d_k + (m:2)\, b_{k-1}^{m-2} d_k^2 p^k + \dots + d_k^m \cdot p^{km-1} = x_k p$$

Looking at this modulo p all except the first two summands vanish:

$$x_{k-1} + m\, b_{k-1}^{m-1} d_k \equiv 0 \pmod p$$

We introduce one factor b_{k-1}

$$b_{k-1} x_{k-1} + m \cdot b_{k-1}^m d_k \equiv 0 \pmod p$$

and because $b_k^m \equiv 1 \pmod p$ for all k we have

$$b_{k-1} x_{k-1} + m\, d_k \equiv 0 \pmod p$$

which allows to determine d_k from the values in the previous step.

(2.4.3) $$d_k \equiv - b_{k-1} x_{k-1} / m \pmod p$$

The modular equation *(2.4.3)* can always be satisfied by a certain d_k where also $0 \le d_k < p$ and thus the assumption is proved by induction.

2.5. Multiple bases for same power of *p*

These digit-vectors transfer the concept of complex unit-roots to the ring of *p-adics*, as is mentioned in several articles on fermat-quotients.

Because a complete sequence of bases for fermat-quotients with increasing powers of *p* can be coded in a single number (in *p*-numbersystem), and this sequence starts at a certain selected residue, we may express the complete set of bases as list of the digits of that numbers beginning at each nontrivial residue. For instance, for *p=7* we have the full matrix of *7–1* rows corresponding to initial residues except the zero (the least significant digit is at the right):

λ		d_{19}	d_{18}	d_{17}	d_{16}	d_{15}	d_{14}	d_{13}	d_{12}	d_{11}	d_{10}	d_9	d_8	d_7	d_6	d_5	d_4	d_3	d_2	d_1	d_0
–		–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	0
1	…	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
3	…	1	6	4	1	2	1	2	5	4	4	3	4	2	6	2	0	3	6	4	2
6	…	1	6	4	1	2	1	2	5	4	4	3	4	2	6	2	0	3	6	4	3
3	…	5	0	2	5	4	5	4	1	2	2	3	2	4	0	4	6	3	0	2	4
6	…	5	0	2	5	4	5	4	1	2	2	3	2	4	0	4	6	3	0	2	5
2	…	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

In the row with $d_0 = 3$ (see last column) with the yellow marked digits we find our just discussed number

$$\text{"2 1 2 5 4 4 3 4 2 6 2 0 3 6 4 3"}_{\text{base 7}} = 10445516265495_{\text{base 10}} = b_{16}$$

and $b_{16}^{6} = 10445516265495^{6} \equiv 1 \pmod{7^{16}}$

where the exponent 6 is taken from the λ-information (in the first column of table) for the initial base 3.

To get another base, which provides a fermat-quotient with same power of *p*, we may select the digits from one of the rows at d_0=*1,2,3,4,5* or *6*, where selections *1* and *6 (=p-1)* may be called trivial solutions.

The nontrivial solutions are then the following *p–3* solutions:

b_0 = Residue	λ	digits base 7	b_{16}	fermat-quotient
2	3	"2 1 2 5 4 4 3 4 2 6 2 0 3 6 4 2"$_7$	10445516265494	$b_{16}^{3} \equiv 1 \bmod(7^{16})$
3	6	"2 1 2 5 4 4 3 4 2 6 2 0 3 6 4 3"$_7$	10445516265495	$b_{16}^{6} \equiv 1 \bmod(7^{16})$
4	3	"4 5 4 1 2 2 3 2 4 0 4 6 3 0 2 4"$_7$	22787414304106	$b_{16}^{3} \equiv 1 \bmod(7^{16})$
5	6	"4 5 4 1 2 2 3 2 4 0 4 6 3 0 2 5"$_7$	22787414304107	$b_{16}^{6} \equiv 1 \bmod(7^{16})$

Completely analoguously this can be done for other primes *p*.

3. Searching primes *p* for given base *b*

3.1. Intro

Much more difficult than the search for a base *b* given a primenumber *p* is the opposite question: find a prime *p* given a base *b* with *fq-order α>1*. For instance, for the base *2* in

$$\{2^{p-1} - 1 , p \} = \alpha > 1$$

we know only two primenumbers *p=1093* and *p=3511* satisfying this description although much computerpower was and is invested in the search. The tables, given in chap *2* and appendix *1* and *2*, may provide an idea about the configuration of the problem, but such tables provide too little data to follow a promising path for any rule underlying the *fq*-order problem.

If we look at table *5.1* in app. *1* and count the number of *α>1* per cycle in the column of one prime, we notice, that for an interval of bases of length p^2 we have *p–1* occurences of an high *α*. So we may say, that for any entry in a column in table *5.1* the likelihood to have an high *α* is $(p-1)/p^2$ or $1/p(1-1/p)$.

The likelihood for a base to have an high alpha in the interval of primes from *p=2* to $p=p_k$ is then some accumulation of these values. Surely, this assumes no further knowledge about the structure of the problem and the modular requirements of the involved numbers. But this simple argument would suggest, that the number of high alphas for a given base is infinite, perhaps with some exceptions, because the sum of reciprocal primes is infinite.

In this view it is surprising, that all effort did not lead to another wieferich prime after G. Beeger had found *p=3511* already in 1922 although primes up to $p \sim 10^{16}$ were checked by various authors *(see [Keller98], [Keller05], [Fischer] for listings of current research results).*

3.2. Increase the database: using composites *n* instead of prime *p*

Approaching the question from an amateurish view the first problem is the small base of data. For every small base we have just a handful of occurences of high *α*'s, if at all, for *b=2* we have only two. So it seems meaningful to extend the problem from primes *p* to general integers *n* and reformulate for a given base *b*:

$$\{b^{\varphi(n)} - 1, n\} > 1$$

where *φ(n)* is the *Euler-totient*-function (or "*phi*"-function) [1].

This shows indeed some structure, however still not really clear. But we find, that there is a certain initial regularity and frequency of high *α*'s and that with increasing *n* that occurences seem to fade out.

For instance, for the base *b=3* we find this way the numbers in the interval *1<n<50000*:

$$n = [11, 22, 44, 55, 110, 220, 440, 880]$$

providing $\alpha_n > 1$ in $\{b^{\varphi(n)} - 1 , n \} = \alpha_n > 1$. These are all multiples of *11*:

$$n = 11 \cdot [\ 1 \cdot (1,2,4),\ \ 5 \cdot (1,2,4,8,16))\ ]$$

[1] This approach was also described and investigated by [Skula]

and the values of the φ –function are

$$\varphi(n) = [10, 10, 20, 40, 40, 80, 160, 320]$$
$$= 10\cdot[1, 1, 2, 4, 4, 8, 16, 32]$$

For base $b=2$ we get for the same search-interval for n

$$n = [1093, 3279, 7651, 14209, 22953, 42627, 3511, 10533, 17555, 31599, 45643]$$
$$=[\, 1093\cdot[1, 3, 7, 13, 3\cdot7, 3\cdot13, ??],$$
$$3511\cdot[1, 3, 5, 3^2, 13, ??]]$$

which have the φ–values:

$$\varphi(n) = [1092\cdot[1, 2, 6, 12, 12, 24, ??],$$
$$3510\cdot[1, 2, 4, 6, 12]\ ]$$

This is a bit better than to see only two values, but still way too few values to see any promising hint.

Interestingly there are some bases which seem to give very few high α's, and other bases giving extremely many; for instance $b=19$ gives a lot of high α; see a full table in appendix 5 where n was checked up to $n=2..50000$.

3.3. Description of tables in appendix 5

Here is the description how to read the tables.

Table for $\{19^{\varphi(n)} - 1\ , n\} > 1$ // gcd(19,n)=1

Base $b=19$, not only primes p but also composites were tested for high fermat-exponent.

n_{odd}	=(primefactors)	$\cdot2^0$	$\cdot2^1$	$\cdot2^2$	$\cdot2^3$	$\cdot2^4$	$\cdot2^5$			3	7	13	17	43	137
3	3	1	2	4						1					
7	7	1	2	4							1				
13	13	1	2	4	8							1			
21	3.7	1	2	4	8					1	1				
39	3.13	1	2	4	8	16				1		1			
43	43	1	2	4										1	

We have data for $\{19^{\varphi(n)} - 1\ ,\ n\} = \alpha_n$; if we get $\alpha_n > 1$ for some n, then this n is listed.

We find in the column n_{odd}, that $n=3,\ n=7\ ,\ n=13,\ n=21,\ n=39,\ n=43$ satisfy the description. Also $n=3,7,13$ and 43 are primes, thus restating known results *(see [Fischer] for instance)*.

But also some even multiples provide high α; these are listed in the columns with the powers of 2. We have, that also $n=3$, $n=3\cdot2=6$ and $n=3\cdot4=12$ provide high α, but also $n=39$, $n=78(=39\cdot2)$, $n=156\ (=39\cdot4)$, $n=312\ (=39\cdot8)$ and $n=624\ (=39\cdot16)$.

The primefactor-decomposition of n_{odd} is in the second column in a string-format and in the righthand columns in separated format.

Two animating observations:

1) the primes in the primefactor-decomposition seem to have some relation to the base, and
2) although we increase n up to 50000 the sequence of even multiples of the primes and odd composites ***fades out*** already at low powers of their primefactors 2. On the other hand we see, that while small primefactor may fade out with some bases high primefactors occur later if n is increased.

3.4. Systematizing some observations

What we empirically see is, that if an n contains a power of 2, such that $n=x\cdot 2^m$, then all $n \in x \cdot [\ 2^0,2^1,2^2,\ldots 2^m]$ are in the list too. Similarly this seems to be the case for at least some other primefactors.

Assume n as a power of a prime, say $n=p^m$. Assume then that we have a base b providing

$$b^{\varphi(p^m)} - 1 = x_1 (p^m)^2 = x_1 p^{2m}$$

Then we look at the same relation with a reduced m:

$$b^{\varphi(p^{m-1})} - 1 = x_2 (p^{m-1})^2 = x_2 p^{2m-2}$$

But we know also, that if

$$b^{\varphi(p)\,p^m} - 1 = x_1 p^{\alpha} \qquad \text{with } \alpha>0 \text{ then} \qquad b^{\varphi(p)pp^m} - 1 = x_2 p^{\alpha+1}$$

If we plug this into the above formula we get

$$b^{\varphi(p)p^{m-1}} - 1 = x_1 p^{2m}$$
$$b^{\varphi(p)p^{m-2}} - 1 = x_2 p^{2m-1} = x_2 p^{2m-2}\cdot p$$

So we can say:

$$\begin{array}{lll} \text{given } n = p^m & & \\ \text{if} & \{b^{\varphi(n)} - 1,\ n^2\} = \alpha & > 0 \\ \text{then} & \{b^{\varphi(n/p)} - 1,\ (n/p)^2\} & = \alpha+1 \\ & \{b^{\varphi(n/p^2)} - 1,\ (n/p^2)^2\} & = \alpha+2 \\ & \ldots & \\ & \{b^{\varphi(p)} - 1,\ p^2\} & = \alpha+m-1 \end{array}$$

Verbally, this effect is:

> For a given base b if we find some $n_m=p^m$ dividing $b^{\varphi(n_m)}-1$ by its square, then all $n_1, n_2, \ldots , n_m$ are in the table.

This explains the effect for cases, where n is a perfect power of a prime. For other composite n this relation is trickier since the exponent at b "mangles" factors of n_m and of $\varphi(n_m)$ in a complicated way.

3.5. Example : Wieferich primes and composites, base $b=2$

To look at it in an example where the situation is not too complicated, I give the results for base $b=2$ and all composites n satisfying

$$\{b^{\varphi(n)} - 1,\ n^2\} = \alpha_n > 0$$

based on the wieferich-primes $p_1=1093$, $p_2=3511$ and the primefactors of their $\varphi()$-values.

Here ***only*** p_1 and p_2 occur as single primefactors while the primefactors of their $\varphi()$-values occur only in conjunction with p_1 or p_2. For this reason a distinction between ***"independent~"*** and ***"dependent primes"*** seems to be meaningful.

Moreover, it seems interesting that p_1 and p_2 can occur also jointly.

Base $b=2$; independent primes: 1093, 3511, dependent primes $13,7,5,3$ (are the primefactors of $\varphi(1093)$ and $\varphi(3511)$.

$$\begin{aligned}
\varphi(1093) &= 13 \cdot 7 \cdot 3 \cdot 2^2 \\
\varphi(13) &= 3 \cdot 2^2 \\
\varphi(7) &= 3 \cdot 2 \\
\varphi(3) &= 2
\end{aligned}$$

$$\begin{aligned}
\varphi(3511) &= 13 \cdot 5 \cdot 3^3 \cdot 2 \\
\varphi(13) &= 3 \cdot 2^2 \\
\varphi(5) &= 2^2 \\
\varphi(3) &= 2
\end{aligned}$$

We have $\alpha_n>0$ for some composites n, according to the following primefactor-decompositions. For brevity I collected consecutive entries, for instance in the first row it means we have $n = 1093^1 \cdot 3^0$ and $n=1093^1 \cdot 3^1$ as valid composites, such that $2^{\varphi(n)} - 1 \equiv 0 \pmod n$ and the last row means, we have all

$$n = 3511^1 \cdot 1093^1 \cdot 13^2 \cdot 7 \cdot 5^0 \cdot 3^k \text{ for } k=0,1,2,3,4,5,6$$

and $$n = 3511^1 \cdot 1093^1 \cdot 13^2 \cdot 7 \cdot 5^1 \cdot 3^k \text{ for the same range of } k$$

Table: Compositions for n, such that $\{2^{\varphi(n)} - 1 , n\} > 1$. Only displayed primefactors were checked.

3511	1093	13	7	5	3
	1	0	0		0..1
	1	0	1		0..2
	1	1	0		0..2
	1	1	1		0..3
1		0		0..1	0..3
1		1		0..1	0..4
1	1	0	0	0..1	0..4
1	1	1	0	0..1	0..5
1	1	2	0	0..1	0..5
1	1	0	1	0..1	0..5
1	1	1	1	0..1	0..6
1	1	2	1	0..1	0..6

See more tables in appendix *6*

Possibly we find another Wieferich prime if we search for one, which has *1093* as factor in its Euler-phi-function…

Gottfried Helms, 3'2017 (3'2012, 8'2009)

4. References:

[1][Keller98] Fermat quotients $q_p(a)$ that are divisible by p
Wilfrid Keller and Jörg Richstein
http://www1.uni-hamburg.de/RRZ/W.Keller/FermatQuotient.html

[Keller05] Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$
Wilfrid Keller and Jörg Richstein.
Journal: Math. Comp. **74** (2005), 927-936.

Abstract: To supplement existing data, solutions of $a^{p-1} \equiv 1 \pmod{p^r}$ are tabulated for primes a,p with $100<a<1000$ and $10^4<p<10^{11}$.

For $a<100$, five new solutions $p>2^{32}$ are presented.

One of these, $p=188748146801$ for $a=5$, also satisfies the "reverse" congruence $p^{a-1} \equiv 1 \pmod{a^2}$. An effective procedure for searching for such "double solutions" is described and applied to the range $a<10^6$, $p<\max(10^{11},a^2)$. Previous to this, congruences $a^{p-1} \equiv 1 \pmod{p^r}$ are generally considered for any $r \geq 2$ and fixed prime p to see where the smallest prime solution a occurs.

[2][sbb] (online-discussion in sbb-forum)
http://www.hamiel.de/cgi-bin/sbb.cgi?&a=show&forum=6&show=1&start=0

[3][Fischer] Fermat quotient
Richard Fischer, 2008
http://www.fermatquotient.com/

[Mathworld] Fermat quotient
Eric Weissstein
http://mathworld.wolfram.com/FermatQuotient.html

[PrimePages] Fermat quotient
Chris Caldwell
http://primes.utm.edu/glossary/page.php?sort=FermatQuotient

Further readings:

[BankLuSh] Estimates for Wieferich Numbers
William D. Banks, Florian Luca, Igor E. Shparlinski
The Ramanujan journal, 2007, Vol 14, No 3,
Springer, Heidelberg
http://www.springerlink.com/content/j747t374h5535884/
(there was also a free version online, don't know the current status)

[Yamada] On Wieferich primes and p-adic logarithms
Tomohiro Yamada
July 4, 2006
arXiv:math.NT/0607072 v3
http://arxiv.org/PS_cache/math/pdf/0607/0607072v3.pdf

Abstract: We shall make a slight improvement to a result of p-adic logarithms which gives a nontrivial upper bound for the exponent of p dividing the Fermat quotient x^{p-1}.

[Skula] Fermat and Wilson Quotients for P-Adic Integers
Ladislav Skula
Acta Mathematica et Informatica Universitatis Ostraviensis 6 (1998) 167-181
online: http://dml.cz/bitstream/handle/10338.dmlcz/120531/ActaOstrav_06-1998-1_21.pdf

See also a directory of more online-links and references at
http://go.helms-net.de/math/expdioph/fermatquotient/directory

Search also for keyword: "wieferich-primes"

My math-projects-pages (Mathematical Miniatures):

[Helms] http://go.helms-net.de/math

5. Appendices

5.1. Appendix 1: table of lengthes λ and cyclicity of α for small bases and primes

Lists of α and λ for the primes *2..47* in $b^n-1 \pmod p$ for some small b. The entries are "α_λ" (if $\alpha=1$ only "λ" is documented). So we see, for instance in the column of prime $p=11$ and row 3^n-1 the entry *2_5*, which means $3^5 - 1 \equiv 0 \pmod{11^2}$. The boxes focus the cyclicitiness in cyclelentghes of p and p^2; in a pair of soft and strong color (for instance at $p=5$, 7^n-1 and 18^n-1) the bases sum up to p.

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	...	1093
1^n-1:	?	1	1	1	1	1	1	1	1	1	1	1	1	1	1		1
2^n-1:	.	2	4	3	10	12	8	18	11	28	5	36	20	14	23		2_364
3^n-1:	1	.	4	6	2_5	3	16	18	11	28	30	18	8	42	23		
4^n-1:	.	1	2	3	5	6	4	9	11	14	5	18	10	7	23		
5^n-1:	2_1	2	.	6	5	4	16	9	22	14	3	36	20	42	46		
6^n-1:	.	.	1	2	10	12	16	9	11	14	6	4	40	3	23		
7^n-1:	1	1	2_4	.	10	12	16	3	22	7	15	9	40	6	23		
8^n-1:	.	**2_2**	4	1	10	4	8	6	11	28	5	12	20	14	23		
9^n-1:	3_1	.	2	3	2_5	3	8	9	11	14	15	9	4	21	23		
10^n-1:	.	2_1	.	6	2	6	16	18	22	28	15	3	5	21	46		
11^n-1:	1	2	1	3	.	12	16	3	22	28	30	6	40	7	46		
12^n-1:	.	.	4	6	1	2	16	6	11	4	30	9	40	42	23		
13^n-1:	2_1	1	4	2	10	.	4	18	11	14	30	36	40	21	46		
14^n-1:	.	2	2	.	5	1	16	18	22	2_28	15	12	8	21	23		
15^n-1:	1	.	.	1	5	12	8	18	22	28	10	36	40	21	46		
16^n-1:	.	1	1	3	5	3	2	9	11	7	5	9	5	7	23		
17^n-1:	4_1	**2_2**	4	6	10	6	.	9	22	4	30	36	40	21	23		
18^n-1:	.	.	2_4	3_3	10	4	1	2	11	28	15	2_36	5	42	23		
19^n-1:	1	2_1	2	3_6	10	2_12	8	.	22	28	15	36	40	2_42	46		
20^n-1:	.	2	.	2	5	12	16	1	22	7	15	36	20	42	46		
21^n-1:	2_1	.	1	.	2	4	4	18	22	28	30	18	20	7	23		
22^n-1:	.	1	4	1	.	2_3	16	18	2	14	30	36	40	14	46		
23^n-1:	1	2	4	3	1	2_6	16	9	.	7	10	12	10	21	46		
24^n-1:	.	.	**2_2**	6	10	12	16	9	1	7	30	36	40	21	23		
25^n-1:	3_1	1	.	3	5	2	8	9	11	7	3	18	10	21	23		
26^n-1:	.	**3_2**	2_1	6	5	.	8	3	11	28	6	3	40	42	46		
27^n-1:	1	.	4	2	2_5	1	16	6	11	28	10	6	8	14	23		
28^n-1:	.	3_1	4	.	10	12	16	2_9	2_22	2	15	18	40	42	23		
29^n-1:	2_1	2	2	1	10	3	16	18	11	.	10	12	40	42	46		
30^n-1:	.	.	.	2_3	10	6	4	3	22	1	2	18	40	42	46		
31^n-1:	1	1	1	2_6	5	4	16	6	11	28	.	4	10	21	46		
32^n-1:	.	2	2_4	3	2	12	8	18	11	28	1	36	4	14	23		
33^n-1:	5_1	.	4	6	.	12	2	18	22	14	5	9	20	42	46		
34^n-1:	.	1	2	2	1	4	.	18	22	14	30	9	40	42	23		
35^n-1:	1	**2_2**	.	.	10	3	1	9	11	14	5	36	40	7	46		
36^n-1:	.	.	1	1	5	6	8	9	11	7	3	2	20	3	23		
37^n-1:	2_1	2_1	4	3	5	12	16	2	22	28	6	.	5	6	23		
38^n-1:	.	2	4	6	5	2	2_4	.	22	14	15	1	8	21	46		
39^n-1:	1	.	2	3	10	.	16	1	11	28	5	36	20	14	46		
40^n-1:	.	1	.	6	2_10	1	2_16	18	22	28	15	18	2	21	46		
41^n-1:	3_1	2	1	2	10	12	16	18	11	2_4	15	18	.	7	46		
42^n-1:	.	.	4	.	5	3	8	9	3_22	14	30	36	1	2	23		
43^n-1:	1	1	2_4	1	2	6	8	9	22	28	30	4	20	.	46		
44^n-1:	.	**2_2**	2	3	.	4	16	9	22	28	30	9	8	1	46		
45^n-1:	2_1	.	.	6	1	12	16	3	2	7	15	12	10	14	46		
46^n-1:	.	2_1	1	3	10	12	16	6	.	4	10	9	20	42	2		
47^n-1:	1	2	4	6	5	4	4	9	1	28	5	3	40	7	.		
48^n-1:	.	.	4	**2_2**	5	3	16	18	11	28	30	6	40	42	1		
49^n-1:	4_1	1	**2_2**	.	5	6	8	3	11	7	15	9	20	3	23		
50^n-1:	.	2	.	2_1	10	12	2	6	11	28	15	36	4	6	23		
51^n-1:	1	.	2_1	3	10	2	.	18	22	14	15	12	2_5	14	23		
52^n-1:	.	1	4	6	10	.	1	18	11	7	30	36	40	21	46		
53^n-1:	2_1	**3_2**	4	3	5	1	8	18	22	7	30	9	40	21	2_23		
54^n-1:	.	.	2	6	2	12	16	2_9	11	7	10	36	40	7	23		

55^n-1:	1	3_1	.	2	.	3	4	9	11	28	30	36	8	42	23		
56^n-1:	.	2	1	.	1	6	16	2	22	28	3	36	40	21	23		
57^n-1:	3_1	.	3_4	1	10	4	16	.	22	2	6	36	5	21	46		
58^n-1:	.	1	4	3	5	12	16	1	11	.	10	18	40	21	46		
59^n-1:	1	2	2	6	5	12	8	18	11	1	15	36	5	7	23		
60^n-1:	.	.	.	3	5	4	8	18	22	2_28	10	12	40	21	46		
61^n-1:	2_1	1	1	6	10	3	16	9	22	28	2	36	20	42	23		
62^n-1:	.	2_2	4	2	10	6	16	2_9	11	14	.	18	20	42	46		
63^n-1:	1	.	4	.	10	12	16	9	2_22	2_14	1	3	40	42	23		
64^n-1:	.	2_1	2	1	5	2	4	3	11	14	5	6	10	7	23		
65^n-1:	6_1	2	.	3	2	.	2_16	6	22	7	30	18	40	14	23		
66^n-1:	.	.	1	6	.	1	8	9	22	28	5	12	10	21	46		
67^n-1:	1	1	4	2_3	1	12	2	18	22	14	3	18	40	21	2_46		
68^n-1:	.	2	3_4	2_6	10	3	.	2_3	2	28	6	4	8	21	23		
69^n-1:	2_1	.	2	2	5	6	1	2_6	.	28	15	36	40	42	46		
70^n-1:	.	1	.	.	5	2_4	8	18	1	4	5	9	40	14	46		
71^n-1:	1	2_2	1	1	5	12	16	18	11	14	15	9	40	42	2_23		
72^n-1:	.	.	4	3	10	12	4	18	11	28	15	36	10	42	23		
73^n-1:	3_1	2_1	4	6	10	4	16	9	11	28	30	2	4	42	46		
74^n-1:	.	2	2_2	3	10	3	16	9	22	7	30	.	20	21	23		
75^n-1:	1	.	.	6	5	6	2_16	2	11	4	30	1	40	2_14	23		
76^n-1:	.	1	2_1	2	2	12	8	.	22	28	15	2_36	40	42	46		
77^n-1:	2_1	2	4	.	.	2	8	1	11	28	10	18	20	42	46		
78^n-1:	.	.	4	1	1	.	16	18	11	7	5	18	5	2_7	46		
79^n-1:	1	1	2	2_3	10	1	16	18	22	28	30	36	8	3	23		
80^n-1:	.	4_2	.	2_6	5	2_12	16	9	22	14	15	4	20	6	46		
81^n-1:	4_1	.	1	3	2_5	3	4	9	11	7	15	9	2	21	23		
82^n-1:	.	4_1	2_4	6	5	6	16	9	11	7	15	12	.	14	46		
83^n-1:	1	2	4	2	10	4	8	3	22	7	30	9	1	21	23		
84^n-1:	.	.	2	.	10	12	2	6	22	28	30	3	20	7	23		
85^n-1:	2_1	1	.	1	10	12	.	9	11	28	10	6	8	2	46		
86^n-1:	.	2	1	3	5	4	1	18	22	2	30	9	10	.	46		
87^n-1:	1	.	4	6	2	3	8	3	11	.	3	36	20	1	46		
88^n-1:	.	1	4	3	.	6	16	6	22	1	6	12	40	14	46		
89^n-1:	3_1	2_2	2	6	1	2_12	4	18	22	28	10	36	40	42	23		
90^n-1:	.	.	.	2	10	2	16	18	22	28	15	9	20	7	46		
91^n-1:	1	1	1	.	5	.	16	18	2	14	10	36	4	42	46		
92^n-1:	.	2	4	1	5	1	16	9	.	14	2	36	5	3	46		
93^n-1:	2_1	.	2_4	3	5	12	8	9	1	14	.	36	40	6	2		
94^n-1:	.	1	2	6	2_10	3	8	2	11	7	1	36	40	14	.		
95^n-1:	1	2	.	3	10	6	16	.	11	28	5	18	40	21	1		
96^n-1:	.	.	1	6	10	4	16	1	11	14	30	36	8	21	23		
97^n-1:	5_1	1	4	2_2	5	12	16	18	22	28	5	12	40	7	23		
98^n-1:	.	2_2	4	.	2	12	4	18	11	28	3	36	5	42	23		
99^n-1:	1	.	2_2	1	.	2_4	16	2_9	22	4	6	18	40	21	46		
100^n-1:	.	1	.	3	1	3	8	9	11	14	15	3	5	21	23		

The primefactor *p=1093* is shown for base *b=2* at 2^n-1 the value *2* in *2_364* indicating it as a Wieferich-prime.

Moreover, since at base $b_0=2$ we have $b_0^{364} \equiv b_0^{1093-1} \equiv 1 \pmod{1093^2}$ we expect the same at base $b_1=1093^2-2=1194647$: and expect

$$b_1^{1093-1} \equiv 1 \pmod{1093^2}$$
$$1194647^{1092}-1 \equiv 1 \pmod{1093^2}$$

which a software like Pari/GP can easily show to be true.

5.2. Appendix 2: Lists of digitstrings for some primes

All tables are to be read with least significant digit from the right; the digits are of the numbersystem of base p.

The base $b_{p,\alpha}$ in $b_{p,k}^{\lambda} - 1 \equiv 0 \pmod{p^{\alpha}}$ has to be composed as translation of the concatenated digits $b_{p,\alpha} = convert("d_{k-1}\, d_{k-2} \ldots d_1\, d_0")$ up to a certain highest index $k=\alpha$.

For $p=3$, using the first table, we get thus subsequently:

$p=3$ Initial residueclass $= b_{3,1} = 2$ ➔ $\lambda=2$

$b_{3,1} = 2_{\text{base } 3} = 2$ $\quad b_{3,1}^{\lambda} - 1 = 2^2 - 1 = 1 \cdot 3^1$

$b_{3,2} = 22_{\text{base } 3} = 8$ $\quad b_{3,2}^{\lambda} - 1 = 8^2 - 1 = 7 \cdot 3^2$

$b_{3,3} = 222_{\text{base } 3} = 26$ $\quad b_{3,2}^{\lambda} - 1 = 26^2 - 1 = 25 \cdot 3^3$

…

For $p=5$ we get thus subsequently:

$p=5$ Initial residueclass $= b_{3,1} = 2$ ➔ $\lambda=4$

$b_{5,1} = 2_{\text{base } 5} = 2$ $\quad b_{5,1}^{\lambda} - 1 = 2^4 - 1 = 3 \cdot 5^1$

$b_{5,2} = 12_{\text{base } 5} = 7$ $\quad b_{5,2}^{\lambda} - 1 = 7^4 - 1 = 96 \cdot 5^2$

$b_{5,3} = 212_{\text{base } 5} = 57$ $\quad b_{5,3}^{\lambda} - 1 = 57^4 - 1 = 84448 \cdot 5^3$

…

Table 5.2.1: Initial residueclass for all primes p is $b_{p,1} = d_0 = 2$

P	λ	…	d_{16}	d_{15}	d_{14}	d_{13}	d_{12}	d_{11}	d_{10}	d_9	d_8	d_7	d_6	d_5	d_4	d_3	d_2	d_1	d_0
3	2	…	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5	4	…	2	3	1	4	0	2	2	3	0	3	2	4	3	1	2	1	2
7	3	…	1	2	1	2	5	4	4	3	4	2	6	2	0	3	6	4	2
11	10	…	5	5	6	6	4	10	10	8	7	9	3	2	1	9	4	10	2
13	12	…	5	0	7	10	11	0	1	3	7	8	5	2	4	2	2	6	2
17	8	…	16	4	16	6	10	8	10	7	10	5	1	14	9	12	3	9	2
19	18	…	11	8	13	12	11	18	16	16	18	14	10	13	14	4	14	6	2
23	11	…	19	10	13	17	22	10	13	18	8	12	9	2	15	10	21	11	2
29	28	…	3	24	24	7	22	6	1	24	13	11	5	16	19	28	26	2	2
31	5	…	17	2	8	24	15	2	26	13	7	4	14	19	16	26	11	12	2
37	36	…	11	26	9	17	20	6	8	13	5	10	26	17	23	17	32	2	2
41	20	…	36	23	19	26	8	2	38	3	17	38	40	8	29	20	38	5	2
43	14	…	40	41	35	16	36	28	41	7	18	15	4	0	34	42	18	7	2
47	23	…	23	23	19	43	32	33	27	45	15	41	6	40	6	20	30	41	2
53	52	…	5	36	35	37	16	38	15	51	34	36	8	0	7	25	27	19	2
59	58	…	37	24	26	51	19	39	51	55	41	29	43	13	19	39	36	16	2
61	60	…	19	42	8	27	1	36	23	20	6	55	37	12	7	56	40	11	2
67	66	…	17	41	8	10	10	6	22	11	11	11	25	56	54	66	9	20	2
71	35	…	9	53	16	61	57	40	65	53	22	44	42	69	47	67	17	4	2
73	9	…	49	48	72	27	53	38	15	34	64	5	11	11	2	63	10	39	2
79	39	…	49	66	9	37	35	50	12	8	44	49	30	64	76	75	67	38	2
…	…	…																	
1093	364	…	1067	250	66	960	534	136	834	1027	581	395	1009	478	564	227	974	0	2
…	…	…	…																

For the prime $p=1093$ we see a zero at d_1 (marked green), which means, that $2^{\lambda_{2,1}(1093)} - 1$ is not only divisible by p but also by p^2, which makes p a wieferich prime.

See a longer list

$p=3..1601$ at http://go.helms-net.de/math/expdioph/fermatquotient_longlist.htm (1.5 MB (!))

Table 5.2.2: Initial residueclass for all primes p is $b_{p,1} = d_0 = 3$

P	λ	…	d_{19}	d_{18}	d_{17}	d_{16}	d_{15}	d_{14}	d_{13}	d_{12}	d_{11}	d_{10}	d_9	d_8	d_7	d_6	d_5	d_4	d_3	d_2	d_1	d_0
5	4	…	0	4	0	2	1	3	0	4	2	2	1	4	1	2	0	1	3	2	3	3
7	6	…	1	6	4	1	2	1	2	5	4	4	3	4	2	6	2	0	3	6	4	3
11	5	…	10	1	8	0	2	0	7	9	3	6	0	7	8	10	6	3	2	1	0	3
13	3	…	9	12	10	10	4	6	10	2	5	1	8	8	4	4	2	7	9	6	11	3
17	16	…	7	11	10	5	16	11	3	3	16	3	9	10	0	4	11	0	3	2	13	3
19	18	…	15	3	5	2	17	8	4	3	2	6	6	18	1	15	18	16	8	7	16	3
23	11	…	0	7	8	10	22	22	12	7	1	18	12	15	7	21	18	7	17	17	5	3
29	28	…	26	22	28	3	26	12	16	2	1	28	23	6	10	27	15	3	0	27	16	3
31	30	…	27	1	23	22	16	12	2	3	24	17	26	14	29	1	23	2	30	14	20	3
37	18	…	6	35	27	28	36	0	34	31	3	7	13	30	21	17	15	12	18	5	17	3
41	8	…	20	4	39	39	35	4	2	1	25	25	35	25	10	5	33	27	15	27	22	3
43	42	…	26	26	13	5	16	37	41	33	7	5	6	14	30	16	31	32	8	4	6	3
47	23	…	14	44	30	23	30	22	3	39	33	15	13	21	7	29	33	19	23	4	33	3
53	52	…	10	44	18	46	31	23	33	39	46	41	10	11	36	37	31	40	27	50	16	3
59	29	…	29	36	49	44	22	15	30	50	19	1	35	43	19	52	51	35	25	39	5	3
61	10	…	47	27	36	43	21	22	33	9	56	6	15	58	46	5	26	36	35	32	39	3
67	22	…	39	3	43	15	36	42	62	12	51	27	23	65	54	65	49	15	3	34	45	3
71	35	…	70	1	6	39	50	42	48	50	52	28	14	33	42	5	52	63	40	16	25	3
73	12	…	47	23	37	69	64	56	28	58	61	6	23	26	39	28	17	15	54	17	5	3
79	78	…	4	2	55	27	43	12	68	69	19	76	50	23	67	55	47	55	3	35	4	3

5.3. Appendix 3: Proof that "from $\{b-1, p\} = \alpha > 0$ follows $\{b^p - 1, p\} = \alpha + 1$"

Proof that for an odd prime p from $\{b-1, p\} = k > 0$ follows that $\{b^p - 1, p\} = k + 1$

Given that, with an unknown x and $gcd(x,p) = 1$

$$b - 1 = x\, p^k \qquad k>0$$

then it follows

$$b = 1 + x\, p^k$$

$$\begin{aligned} b^p &= (1 + x\, p^k)^p \\ &= 1 + p\, x p^k + p(p+1)/2\, x^2\, p^{2k} + p(p+1)(p+2)/3\, x^3\, p^{3k} + \ldots + x^p\, p^{kp} \end{aligned}$$

$$\begin{aligned} b^p - 1 &= p\, x p^k + p(p+1)/2\, x^2\, p^{2k} + p(p+1)(p+2)/3\, x^3\, p^{3k} + \ldots + x^p\, p^{kp} \\ &= p^{k+1}(x + (p+1)/2\, x^2\, p^k + (p+1)(p+2)/3\, x^3\, p^{2k} + \ldots + x^p\, p^{k(p-1)-1}) \\ &= p^{k+1}(x + p^k ((p+1)/2\, x^2 + (p+1)(p+2)/3\, x^3\, p^k + \ldots + x^p\, p^{k(p-2)-1})) \end{aligned}$$

Here, since p is an odd prime, all summands in the innermost parenthese are integer and we have, with an integer y:

$$\begin{aligned} b^p - 1 &= p^{k+1}(x + p^k\, y) \\ \{ b^p - 1, p\} &= k+1 \end{aligned}$$

which proves, that p occurs in $b^p - 1$ to the $(k+1)$'th power if it occurs in $b - 1$ to the k'th power.

This can also be used for the general expression:

$$\{b^{p^{k+1}} - 1, p\} = \{b^{p^k} - 1, p\} + 1 \qquad \text{if } \{b-1, p\} > 0$$

see also: http://www.mathlinks.ro/Forum/viewtopic.php?t=155890

5.4. Appendix 4: Pari/GP-code-snippets

a) Function to determine the value for $\lambda_{b,1}(p)$:

```
LAMBDA(p,base) = znorder(Mod(base,p)) \\ this is the on-board solution
\\ --- computing this explicitely
{ LAMBDA(p,base) =local(tmp,rs,lam=p-1,testlam,fakv,fakp);
   if(isprime(p)==0,return(0));
   if(base^lam % p <> 1,return(0));   \\ LAMB = 0 means infinity;
                                      \\ residue 1 does never occur
   tmp = factor(p-1); rs = rows(tmp); \\ primefactors of p-1 in tmp
   for(r=1,rs,
         fakv=tmp[r,1];fakp=tmp[r,2];  \\ fakv:value of primefactor
                                       \\ fakp:exponent of this primefactor
         testlam=lam;
         forstep(c=fakp,1,-1,       \\ find smallest lam which still
                                    \\ gives residue 1
             testlam=testlam/fakv;
             if( base^testlam % p <> 1 ,break()); \\ if not residue=1 with
                                                  \\ small testlam exit loop
             lam=testlam;                         \\ testlam is usable
             );
       );
   return(lam); }
```

Comment: Instead of trying each exponent from *1* to *p–1* the function tests just the divisors of *p–1*.

It proceeds from assuming the maximum length *testlam=p–1* and trying for each primefactor *fakv* of *p–1*, whether one power after the other of *facv* can be taken out and the function $b^{testlam} - 1$ still contains the primefactor *p*.

b) Function to determine the value for $\alpha_{b,1}(p)$:

```
{ ALPHA(p,base) =local(lam,tmp);
   if(isprime(p)==0,return(0)); if(gcd(p,base)>1,return(0));
   lam = LAMBDA(p,base);              if(lam==0, return(0));
   tmp=valuation(base^lam - 1, p);    if(tmp<0,  return(0));
   return(tmp); }
```

c) Function to find a base *b* according to a given exponent *k* of *p* in the fermatquotient. The result is given as array of digits in base *p*; you can return the integer base *b* instead.

```
\\ -- the onboard-solution, returns the base b as number
ferquot(p=5,d0=3,maxk=12) = lift(teichmuller(d0 + O(p^maxk)))

\\ the explicite computation, returns the vector of "digits"
{ferquot(p=5,d0=3,maxk=12) = local(b=d0,m,dig,x,dk);
  dig=vector(1+maxk);                 \\ contains the final "digits"
     if(! isprime(p), return(dig));    \\ error
     if( gcd(p,b)>1 , return(dig));    \\ error

  dig[1]=d0;
  m=LAM(p,b);
  for(k=1,maxk,
       x = (b^m - 1)/p^k;
       dk=(- b* x / m  ) % p;
       dig[1+k]=dk;
       b = b + dk*p^k;
      );
  return(dig); }
```

5.5. Appendix 5: composites *n* instead of prime *p* providing high *fq-degree*

(5.5.1) Table for $\{2^{\varphi(n)}-1, n\} = \alpha > 1$ // gcd(2,n)=1

Base *b=2*, not only primes *p* but also composites were tested for high fermat-exponent. In [Skula] it is stated, that these *104* moduli *n* with Euler-quotients*>1* are the only ones below a lower bound given by any (yet unknown) Wieferich prime (*p> 1e15* if it exists)

n_{odd}		$\cdot 2^0$		3	5	7	13	1093	3511
1093	1093	1						1	
3279	3.1093	1		1				1	
7651	7.1093	1				1		1	
14209	13.1093	1					1	1	
22953	3.7.1093	1		1		1		1	
42627	3.13.1093	1		1			1	1	
3511	3511	1							1
10533	3.3511	1		1					1
17555	5.3511	1			1				1
31599	3^2.3511	1		2					1
45643	13.3511	1					1		1

(5.5.2) Table for $\{3^{\varphi(n)}-1, n\} > 1$ // gcd(3,n)=1

Base *b=3*, not only primes *p* but also composites were tested for high fermat-exponent

n_{odd}		$\cdot 2^0$	$\cdot 2^1$	$\cdot 2^2$	$\cdot 2^3$	$\cdot 2^4$	$\cdot 2^5$		5	11	1006003
11	11	1	2	4	0	0					
55	5.11	1	2	4	8	16					

(note: in app 5.6 in the according table the prime *p=1006003* is also included)

(5.5.3) Table for $\{71^{\varphi(n)}-1, n\} > 1$ // gcd(71,n)=1

Base *b=71*, not only primes *p* but also composites n_0 were tested for high fermat-exponent

n_{odd}		$\cdot 2^0$	$\cdot 2^1$	$\cdot 2^2$	$\cdot 2^3$	$\cdot 2^4$	$\cdot 2^5$	2	3	5	11	23	47	331
0	0													
3	3	1	2	4	8				1					
1	2		2					2						
47	47	1	2	4	8								1	
141	3.47	1	2	4	8	16			1				1	
331	331	1	2	4	8									1
993	3.331	1	2	4	8	16			1					1
1081	23.47	1	2	4	8	16						1	1	
1655	5.331	1	2	4	8	16				1				1
2979	3^2.331	1	2	4	8	16			2					1
3243	3.23.47	1	2	4	8				1			1	1	
3641	11.331	1	2	4	8						1			1
4965	3.5.331	1	2	4	8				1	1				1
10923	3.11.331	1	2	4					1		1			1
11891	11.23.47	1	2	4							1	1	1	
14895	3^2.5.331	1	2						2	1				1
15557	47.331	1	2										1	1
18205	5.11.331	1	2							1	1			1
32769	3^2.11.331	1							2		1			1
35673	3.11.23.47	1							1		1	1	1	
46671	3.47.331	1							1				1	1

(5.5.4) Table for $\{19^{\varphi(n)} - 1, n\} > 1$ // gcd(19,n)=1

Base $b=19$, not only primes p but also composites were tested for high fermat-exponent.

n_{odd}			$\cdot 2^1$	$\cdot 2^2$	$\cdot 2^3$	$\cdot 2^4$	$\cdot 2^5$			3	7	13	17	43	137
3	3	1	2	4						1					
7	7	1	2	4							1				
13	13	1	2	4	8							1			
21	3.7	1	2	4	8					1	1				
39	3.13	1	2	4	8	16				1		1			
43	43	1	2	4										1	
49	7^2	1	2	4							2				
63	3^2.7	1	2	4	8					2	1				
91	7.13	1	2	4	8	16					1	1			
117	3^2.13	1	2	4	8	16				2		1			
129	3.43	1	2	4	8					1				1	
137	137	1	2	4	8	16									1
147	3.7^2	1	2	4	8					1	2				1
273	3.7.13	1	2	4	8	16	32			1	1	1			
301	7.43	1	2	4	8						1			1	
387	3^2.43	1	2	4	8					2				1	
411	3.137	1	2	4	8	16	32			1					1
441	3^2.7^2	1	2	4	8					2	2				
559	13.43	1	2	4	8	16						1		1	
637	7^2.13	1	2	4	8	16					2	1			
819	3^2.7.13	1	2	4	8	16	32			2	1	1			
903	3.7.43	1	2	4	8	16				1	1			1	
959	7.137	1	2	4	8	16	32				1				1
1677	3.13.43	1	2	4	8	16				1		1		1	
1781	13.137	1	2	4	8	16						1			1
1911	3.7^2.13	1	2	4	8	16				1	2	1			
2107	7^2.43	1	2	4	8						2			1	
2329	17.137	1	2	4	8	16							1		1
2457	3^3.7.13	1	2	4	8	16				3	1	1			
2709	3^2.7.43	1	2	4	8	16				2	1			1	
2877	3.7.137	1	2	4	8	16				1	1				1
3913	7.13.43	1	2	4	8						1	1		1	
5031	3^2.13.43	1	2	4	8					2		1		1	
5343	3.13.137	1	2	4	8					1		1			1
5733	3^2.7^2.13	1	2	4	8					2	2	1			
5891	43.137	1	2	4	8									1	1
6321	3.7^2.43	1	2	4						1	2			1	
6713	7^2.137	1	2	4							2				1
6987	3.17.137	1	2	4						1			1		1
8127	3^3.7.43	1	2	4						3	1			1	
8631	3^2.7.137	1	2	4						2	1				1
11739	3.7.13.43	1	2	4						1	1	1		1	
12467	7.13.137	1	2	4							1	1			1
14749	7^3.43	1	2								3			1	
15093	3^3.13.43	1	2							3		1		1	
16029	3^2.13.137	1	2							2		1			1
16303	7.17.137	1	2								1		1		1
17199	3^3.7^2.13	1	2							3	2	1			
17673	3.43.137	1	2							1				1	1
18963	3^2.7^2.43	1	2							2	2			1	
20139	3.7^2.137	1	2							1	2				1
27391	7^2.13.43	1									2	1		1	
30277	13.17.137	1										1	1		1
35217	3^2.7.13.43	1								2	1	1		1	
37401	3.7.13.137	1								1	1	1			1
41237	7.43.137	1									1			1	1
44247	3.7^3.43	1								1	3			1	
48909	3.7.17.137	1								1	1		1		1

5.6. Appendix 6: tables with independent and dependent primefactors

The following tables display primefactor-compositions for *n*, such that $\{b^{\varphi(n)} - 1 , n\} = \alpha > 1$. Only compositions of the displayed primefactors were checked. The search-limit for exponents at primefactors *2* and *3* was *12*, at other primefactors *3*

Table 5.6.1: Base *b=2*, independent primes $p_1=1093$, $p_2=3511$

Head row: primefactors, body-rows: exponents for primefactors or range of exponents

3511	1093	13	7	5	3
	1	0	0		0..1
	1	0	1		0..2
	1	1	0		0..2
	1	1	1		0..3
1		0		0..1	0..3
1		1		0..1	0..4
1	1	0	0	0..1	0..4
1	1	1	0	0..1	0..5
1	1	2	0	0..1	0..5
1	1	0	1	0..1	0..5
1	1	1	1	0..1	0..6
1	1	2	1	0..1	0..6

Table 5.6.2 Base *b=3*, independent primes $p_1=11$, $p_2=1006003$

Head row: primefactors, body-rows: exponents for primefactors or range of exponents

1006003	11	55889	499	83	41	7	5	2
	1						0	0..2
	1						1	0..4
1		0	0	0	0	0	0	0..2
1		1	0	0	0	0	0	0..6
1		1	0	0	0	1	0	0..7
1		1	1	0	0	0	0	0..7
1		1	1	0	0	1	0	0..8
1		1	1	1	0	0	0	0..8
1		1	1	1	0	1	0	0..9
1		1	1	1	1	0	0	0..11
1		1	1	1	1	0	1	0..12
1		1	1	1	1	1	0	0..12
1		1	1	1	1	1	1	0..12
1	1	0	0	0	0	0	0	0..3
1	1	0	0	0	0	0	1	0..5
1	1	1	0	0	0	0	0	0..7
1	1	1	0	0	0	0	1	0..9
1	1	1	0	0	0	1	0	0..8
1	1	1	0	0	0	1	1	0..10
1	1	1	1	0	0	0	0	0..8
1	1	1	1	0	0	0	1	0..10
1	1	1	1	0	0	1	0	0..9
1	1	1	1	0	0	1	1	0..11
1	1	1	1	1	0	0	0	0..9
1	1	1	1	1	0	0	1	0..11
1	1	1	1	1	0	1	0	0..10
1	1	1	1	1	0	1	1	0..12
1	1	1	1	1	1	0	0..2	0..12
1	1	1	1	1	1	1	0..2	0..12

Table 5.6.3 Base *b=7*, independent primes $p_1=5$, $p_2=491531$

Head row: primefactors, body-rows: exponents for primefactors or range of exponents

491531	5	199	19	11	3	2
0	1	0	0	0	0	0..4
1	0	0	0	0	0	0..3
1	1..2	0	0	0	0	0..5
1	0	0	1	0	0	0..4
1	0	0	1	0	1..2	0..5
1	1..2	0	1	0	0	0..6
1	1..2	0	1	0	1..2	0..7
1	0	1	0	0	0	0..4
1	0	1	0	0	1..2	0..5
1	1..2	1	0	0	0	0..6
1	1..2	1	0	0	1..2	0..7
1	0	1	0	1	0	0..5
1	0	1	0	1	1..2	0..6
1	1..3	1	0	1	0	0..7
1	1..3	1	0	1	1..2	0..8
1	0	1	1	0	0	0..5
1	0	1	1	0	1..4	0..6
1	1..2	1	1	0	0	0..7
1	1..2	1	1	0	1..4	0..8
1	0	1	1	1	0	0..6
1	0	1	1	1	1..4	0..7
1	1..3	1	1	1	0	0..8
1	1..3	1	1	1	1..4	0..9

Table 5.6.4 Base *b=11*, independent primes $p_1=71$

Head row: primefactors, body-rows: exponents for primefactors or range of exponents

71	7	5	3	2
1	0	0	0	0..2
1	0	1	0	0..4
1	1	0	0	0..3
1	1	0	1	0..4
1	1	1	0	0..5
1	1	1	1	0..6