Some computational experiments in number theory

Wieb Bosma

Mathematisch Instituut
Radboud University Nijmegen
Nijmegen, the Netherlands
`bosma@math.ru.nl`

Summary. The Magma code and some computational results of experiments in number theory are given. The experiments concern covering systems with applications to explicit primality tests, the inverse of Euler's totient function, and class number relations in Galois extensions of $\mathbb{Q}$. Some evidence for various conjectures and open problems is given.

1 Introduction

In the course of 10 years of working with and for Magma [6], I have conducted a large number of computational experiments in number theory. Many of them were meant, at least initially, as tests for new algorithms or implementations. In this paper I have collected results from, and code for, a few of those experiments.

Three main themes can be recognized in the material below: *covering systems*, the *Euler ϕ function*, and *class number relations*.

In section 3 it is shown how covering systems can be used, with cubic reciprocity, to produce a simple criterion for the primality of $n = h \cdot 3^k + 1$ in terms of a cubic recurrence modulo n; the starting value depends only on the residue class of k modulo some covering modulus M. These primality tests generalize the Lucas–Lehmer type tests for numbers of the form $h \cdot 2^k + 1$. They lead to a question about values of h for which $h \cdot 3^k + 1$ is composite for every k, and a generalization of a problem of Sierpiński. We found a 12-digit number h with this property — a candidate analogue for the number 78577, which is most likely the smallest h with the property that $h \cdot 2^k + 1$ is composite for every k. As a simpler application of our methods to produce covering systems in section 2, we improve slightly on the known results for a problem of Erdős; this problem asks for a finite set of congruence classes with distinct moduli, each at least c, that cover all integers.

There is also a connection between Sierpiński's problem and the image of Euler's totient function ϕ; this is explained in section 4, which is devoted to various questions about the ϕ function, its image, its inverse image and its iterates. We describe our implementation of the function that computes all n with $\phi(n) = m$ for a given m; as a test we produced some statistics on the size of the inverse image for the first 327 million even integers. We also experimented extensively with iterates of the composite function $\phi \circ \sigma$, found a new candidate smallest starting value for which this function may not reach a cycle, and recorded many cycles and the frequency with which they occur. We searched for (and found many) new fixed points n, for which $\phi \circ \sigma(n) = n$. For many of the experiments in sections 2–4 the problems and the references collected by Richard K. Guy in [20] proved very valuable.

In section 5 we present some details of computations done with Bart de Smit on relations between class numbers in the subfields of Galois extensions of $\mathbb{Q}$ with some fixed Galois group. This requires computations with transitive permutation groups of small degree and all of their subgroups, and the characters of these groups. Focusing on pairs of fields with the same zeta-function, it is shown how Magma can now deal routinely with questions about the class number quotients for such pairs; in particular, we use resultant computations on polynomial rings over rational function fields to obtain symbolically the explicit defining relations for a family of equivalent number fields in degree 7.

2 Covering systems

A collection of residue classes $a_i \bmod m_i$ is called a *covering system* if every integer n satisfies at least one of the congruences $n \equiv a_i \bmod m_i$. Several constraints in various combinations are possible: for example, one may require the system to be *finite*, to consist of *distinct moduli*, or of *odd moduli* only, or to be *disjoint*. For a finite covering system we will call the least common multiple $M = \mathrm{lcm}\{m_i\}$ of the moduli the *covering modulus*.

A problem of Erdős

Erdős considered the question of whether for all c there exists a covering system with finitely many distinct moduli satisfying $c = m_1 < m_2 < \ldots m_k$ (for some k) to be 'Perhaps my favorite problem of all', and offered \$1000 for a solution [16].

A simple search for solutions for small values of c can be conducted in Magma as follows[⋆].

```
for c := 2 to 10 do
  D := 0;
```

[⋆] See the Preface to this volume for style conventions regarding the Magma code; all code is available also at `http://magma.maths.usyd.edu.au/magma/`

```
    done := FALSE;
    repeat
      D +:= 4;
      S := [ x : x in Divisors(D) | x ge c ];
      if &+[ Integers() | D div s : s in S ] ge D then
        done, F := try(S, D);
      end if;
    until done;
    print < Min([ f[2] : f in F ]), D, F>;
  end for;
```

In this loop one attempts to find solutions with covering modulus D. Only D with many divisors are useful, and this search takes only $D \equiv 0 \bmod 4$ into account. Only if there are enough divisors of D exceeding c to make a covering by residue classes feasible is a call to the function *try* made. The test uses the summation over D **div** s for this, where the specification [Integers() | ...] is used to ensure that the integer 0 is returned when the sum is taken over an empty sequence.

Here is the function *try*:

```
  try := function(S, D)
    Z := Integers();
    for tries := 1 to 50 do
      T := [ ];
      Q := [ 1 : i in [1..D] ];
      for i in [1..#S] do
        addm(~Q, ~T, S[i]);
        if &+[ Z | D div s : s in S[i+1..#S] ] lt &+Q then
          if &+Q/D gt 0.1 then
            break tries;
          end if;
          break;
        elif &+Q eq 0 then
          return TRUE, T;
        end if;
      end for;
    end for;
    return FALSE, _;
  end function;
```

For at most 50 times (a value that could be modified, but which worked well in our experiments) an attempt is made to add one residue class for each modulus (which is a divisor of D) stored in S; this residue class is added to a list (initially empty) that is kept in T. The sequence Q of length D stores 0 in position i precisely when the residue system in T covers the residue class $i-1 \bmod D$ and 1 otherwise. If not enough divisors are left to have any hope of completing the system, this try is aborted and a new one attempted, unless the

50 tries have been completed or the fraction covered in this aborted attempt is so low that the search is abandoned prematurely because it seems hopeless altogether. An attempt is aborted if the cover could not even be completed if all remaining residue classes were disjoint, and this implementation considers the case hopeless (and no more attempt is made) if an aborted attempt occurs when still more than 10% is uncovered.

The procedure *addm* is the most interesting part of this simple search.

```
addm := procedure(~Q, ~T, m)
  if &+Q eq #Q then
    addr(~Q, ~T, 1, m);
  else
    mx := [ &+Q[[i..#Q by m]] : i in [1..m] ];
    mm := Max(mx);
    im := Random([ i : i in [1..#mx] | mx[i] eq mm ]);
    addr(~Q, ~T, im−1, m);
  end if;
end procedure;
```

In it, an attempt is made to find a good residue r for the given modulus m to add to the system *T*; ‘goodness’ is measured in terms of the number of previously uncovered classes modulo D that will be covered when adding $r \bmod m$. This success rate is computed for all possible choices (unless no residue class is covered yet, in which case we may and will just choose the class of one) and among the best a random choice is made. This random aspect of the otherwise ‘greedy’ algorithm makes it useful to have several attempts in *try*.

The function *addr* (that is called but will not be listed here) simply adjusts the sequences *Q* and *T* according to the choice made: newly covered classes $i \bmod D$ get their entry in *Q* replaced by a 0 and the pair (r, m) is appended to *T*.

Example 2.1. The little program described is fairly successful for small values for c. Of course it immediately finds a version of the well-known ‘smallest’ covering with modulus 12 for $c = 2$, such as

$$1 \bmod 2, \quad 2 \bmod 3, \quad 2 \bmod 4, \quad 4 \bmod 6, \quad 0 \bmod 12$$

and for $c = 3$ one obtains a covering using divisors of 120. Already for $c = 4$ this algorithm does better than the deterministic algorithm given in the (very early) work of Churchhouse [14]. He gives a solution with moduli that are divisors of 720, whereas our solution

$$\begin{array}{rrrrr}
1 \bmod 4, & 1 \bmod 5, & 4 \bmod 6, & 3 \bmod 8, & 8 \bmod 10, \\
0 \bmod 12, & 14 \bmod 15, & 15 \bmod 16, & 2 \bmod 20, & 18 \bmod 24, \\
20 \bmod 30, & 7 \bmod 32, & 30 \bmod 40, & 7 \bmod 48, & 32 \bmod 60, \\
55 \bmod 80, & 87 \bmod 96, & 54 \bmod 120, & 87 \bmod 160, & 23 \bmod 240,
\end{array}$$

uses divisors of 480. The other values found are listed in the table below, and compared to those obtained by Churchhouse:

2	3	4	5	6	7	8	9	10
12	120	480	2520	5040	20160	60480	151200	1663200
12	120	720	2520	10080	30240	75600	604800	–

For $c = 10$ we found a covering modulus 1663200; we did not find any cover for this case elsewhere in the literature. Note that the values are not necessarily smallest possible, although we tried fairly hard to beat them.

At this stage the method of storing an indicator for every residue class becomes cumbersome. Some larger examples were constructed by Choi [13] and Morikawa [29].

The conjecture of de Polignac

Covering systems were introduced by Erdős, and used by him to give a disproof of a conjecture made in [33] (and quickly retracted; cf. [19]) by de Polignac, namely that every odd $n > 1$ can be written as $2^k + p$ for some k and some prime number p. De Polignac himself had already found small counterexamples; $k = 127, 149, 251$ are the smallest, and there are 14 others below 1000. But the disproof by Erdős exhibits an arithmetic progression of counterexamples, by noting that covering systems $\{r_i \bmod m_i\}$ like

$$0 \bmod 2, \quad 0 \bmod 3, \quad 1 \bmod 4, \quad 3 \bmod 8, \quad 7 \bmod 12, \quad 23 \bmod 24$$

can be used for this purpose. Indeed, observing that the moduli m_i here are equal to the multiplicative order e_i of 2 modulo p_i, where p_i is $3, 7, 5, 17, 13$ or 241 respectively, we see that if we choose simultaneously

$$N \equiv 2^{r_i} \bmod p_i$$

for all classes $r_i \bmod m_i$ in the cover, then for every integer k there exists at least one i for which $k \equiv r_i \bmod m_i$ and hence $N - 2^k \equiv 0 \bmod p_i$; that is, $N - 2^k$ is divisible by p_i. As it is easy to see (by working modulo 31, for example) that $N - 2^k$ cannot be *equal* to p_i, we see that this N gives rise to a counterexample to the conjecture, as does every odd integer in the arithmetic progression of N with modulus $Q = \prod_i p_i = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$. The covering system above yields $N = 2036812$ as the smallest non-negative solution (by application of the Chinese Remainder Theorem) and 7629217 as the smallest counterexample:

```
>   m := [ 0, 0, 1, 3, 7, 23 ];
>   P := [ 3, 7, 5, 17, 13, 241 ];
>   N := CRT([ 2^j : j in m ], P); N;
        2036812
```

The additional condition that m is odd produces the smallest counterexample.

```
>     N + &*P;
        7629217
```

The problems of Sierpiński and Riesel

The fact that $N-2^k$ is always divisible by one of the primes $3, 5, 7, 13, 17, 241$ is closely related to the solution of another problem, concerning the existence of integers H such that $H\cdot 2^k+1$ is composite for every $k \geq 0$. Sierpiński showed that there is an infinitude of such H. Indeed, if we let $Q = 3\cdot 5\cdot 7\cdot 13\cdot 17\cdot 241$ again, then

$$N - 2^k \equiv 0 \bmod p_i \qquad \Longleftrightarrow \qquad H \cdot 2^k + 1 \equiv 0 \bmod p_i,$$

if we let H be such that $H \equiv -N^{-1} \bmod Q$.

In the current example, we let H be the smallest positive element in this residue class and find:

```
>   Q := &*P; Q;
      5592405

>   H := InverseMod(-N, Q); H;
      1624097
```

and the output of

```
>   for k := 0 to 100 do
>     print k, [ p : p in P | (H*2^k+1) mod p eq 0 ];
>   end for;
```

will demonstrate that $H \cdot 2^k + 1$ is divisible by 3 when $k \equiv 0 \bmod 2$, divisible by 7 when $k \equiv 0 \bmod 3$, by 5 when $k \equiv 1 \bmod 4$, etc.

Since there are, in general, several covering systems for a fixed covering modulus, there will be several pairs of solutions N, H as above. The smallest H with covering modulus 24 is $H = 271129$.

However, there exists a smaller integer H with the property that $H\cdot 2^k+1$ is divisible by at least one prime in a fixed, finite collection, but it comes from a covering system with covering modulus 36: the covering system

$$0 \bmod 2,\ 2 \bmod 3,\ 3 \bmod 4,\ 1 \bmod 9,\ 9 \bmod 12,\ 13 \bmod 18,\ 25 \bmod 36$$

yields $N = 20512783$, and $H = 314228$, the odd part of which is 78557.

The problem of determining the smallest H such that $H \cdot 2^k + 1$ is always composite is sometimes referred to as *Sierpiński's problem.* The number $H = 78557$ is the most likely candidate for Sierpiński's problem; see [42] for progress on the remaining work on proving that for every smaller h there is a prime of the form $h \cdot 2^k + 1$. It has been conjectured (but never been proven, as far as I know) that every H such that $H \cdot 2^k + 1$ is always composite arises from a finite covering system.

The similar problem of determining the smallest H such that $H \cdot 2^k - 1$ is always composite is sometimes referred to as *Riesel's problem*; Riesel [36] first showed the existence of infinitely many such H. The most likely candidate is $H = 509203$; see [43].

Note that a Sierpiński number H with covering modulus D also provides a Riesel number $D - H$.

3 Covering systems and explicit primality tests

One way in which the problems of Sierpiński and Riesel (and a generalization) arose naturally for me occurred in [3], and [4]. In these papers the well-known Lucas–Lehmer type tests for $2^n \pm 1$ were generalized to numbers of the form $h \cdot 2^n \pm 1$ and $h \cdot 3^n \pm 1$ using covering systems. We will first explain the connection, and then return to the problems of Sierpiński and Riesel and their generalization.

Non-residue covers

In [3], covering systems were used to solve the following problem: for fixed h find a finite *quadratic non-residue cover* of elements $c_1, c_2, \ldots, c_m \in \mathbb{Z}^*$ satisfying

$$\left(\frac{c_r}{h \cdot 2^k + 1}\right)_2 \neq 1, \quad \text{when} \quad 2 \leq k \equiv r \bmod m.$$

Here the symbol $\left(\text{-}\right)_2$ on the left is the Jacobi symbol. It turns out that such a finite cover can usually be found, unless h is of the form $h = 4^s - 1$. The reason it is of interest to find such a finite cover is the following result.

Theorem 3.1. *If $c_1, \ldots, c_m$ forms a quadratic non-residue cover and $2^k > h$ then, with $k \equiv r \bmod m$:*

$$n = h \cdot 2^k + 1 \quad \textit{is prime} \quad \Longleftrightarrow \quad c_r^{(n-1)/2} \equiv -1 \bmod n.$$

So a quadratic non-residue cover for h provides a nice, very explicit, primality test for the family $h \cdot 2^k + 1$ (for fixed h). The classical example for this is the case where $h = 1$, since in this case $m = 1$ and $c_1 = 3$ work: we get a well-known test for Fermat numbers

$$n = 2^k + 1 \quad \text{is prime} \quad \Longleftrightarrow \quad 3^{(n-1)/2} \equiv -1 \bmod n.$$

In fact, this cover works for any h not divisible by 3.

Similar, but slightly more complicated tests based on covering systems can be derived for families $h \cdot 2^k - 1$, again for h not of the form $4^s - 1$. The extra complication amounts to the following: The cover does not consist of integers c_r but of pairs (D_r, α_r), $r = 1, \ldots, m$, where D_r is an integer discriminant $0 < D_r \equiv 0, 1 \bmod 4$ and α_r is an element of the quadratic field $\mathbb{Q}(\sqrt{D_r})$. These pairs have the property

$$\left(\frac{D_r}{h \cdot 2^k - 1}\right)_2 \neq 1 \quad \text{and} \quad \left(\frac{\alpha_r \bar{\alpha}_r}{h \cdot 2^k - 1}\right)_2 \neq 1 \quad \text{whenever} \quad 2 \leq k \equiv r \bmod m;$$

here $\bar{}$ is the non-trivial $\mathbb{Q}$-automorphism of the quadratic field. Again, this provides explicit primality tests for families $h \cdot 2^k - 1$, which can be formulated either in terms resembling Theorem 3.1 above

$$n = h \cdot 2^k - 1 \quad \text{is prime} \qquad \Longleftrightarrow \qquad \left(\frac{\alpha_r}{\bar{\alpha}_r}\right)^{(n+1)/2} \equiv -1 \bmod n,$$

or in terms of a recurrence relation

$$n = h \cdot 2^k - 1 \quad \text{is prime} \qquad \Longleftrightarrow \qquad e_{k-2} \equiv 0 \bmod n,$$

where $e_{j+1} = e_j^2 - 2$ for $j \geq 0$, and the starting value e_0 is determined by α_r. The classical Lucas–Lehmer case (for Mersenne numbers) is $h = 1$, where again the length of the cover is $m = 1$ and the single pair $(12, 2 + \sqrt{12})$ works; in this case the starting value e_0 equals -4.

The connection with ordinary congruence covers is as follows. Since the Jacobi symbol is multiplicative (in the top argument), it is not a restriction to assume that the c_r are prime. Then I claim that for prime c

$$\left(\frac{c}{h \cdot 2^k + 1}\right)_2 \neq 1 \quad \Longrightarrow \quad \left(\frac{c}{h \cdot 2^j + 1}\right)_2 \neq 1 \quad \text{for every} \quad j \equiv k \bmod d,$$

where d is the multiplicative order of 2 mod c. This is clear from quadratic reciprocity and the fact that $h \cdot 2^k + 1 \equiv h \cdot 2^{k+d} + 1 \bmod c$. So any good pair (c, k) provides a solution for the whole residue class k mod d. The aim in our search for a quadratic non-residue cover then simply becomes that of finding a congruence cover using such residue classes k mod d. The dependence of the modulus d on (the prime) c is that c is a primitive divisor of $2^d - 1$; that is, c divides $2^d - 1$ but not $2^i - 1$ for any value of $i < d$. In other words, d is the multiplicative order of 2 modulo c. The way k and c are related depends on h. For prime $c > 2$ precisely $(c+1)/2$ residue classes modulo c consist of non-residues, so those values k mod d can be used for which $h \cdot 2^k + 1$ mod c is such quadratic non-residue class.

What we would like to show here is how Magma was used [4] to generalize these results to integers of the form $h \cdot 3^k + 1$ using cubic non-residue covers.

Cubic reciprocity

Let $\zeta = \zeta_3$ be a primitive third root of unity. For prime $\pi \in \mathbb{Z}[\zeta]$ with $n =$ Norm $\pi \neq 3$, we let $\left(\frac{\alpha}{\pi}\right)_3$ be the element of $\{0, 1, \zeta, \zeta^2\} \subset \mathbb{Z}[\zeta]$ defined as follows. If π divides α then the value is 0, in all other cases it is the element ζ^i satisfying $\alpha^{\frac{n-1}{3}} \equiv \zeta^i \bmod \pi$.

As a consequence, for $\alpha \in \mathbb{Z}[\zeta]$ and prime $\pi \in \mathbb{Z}[\zeta]$ of norm $n > 3$:

$$\alpha^{\frac{n-1}{3}} \not\equiv 1 \bmod \pi \qquad \Longleftrightarrow \qquad \forall\, x \not\equiv 0 : \; x^3 \not\equiv \alpha \bmod \pi \qquad \Longleftrightarrow \qquad \left(\frac{\alpha}{\pi}\right)_3 \neq 1.$$

Next, one extends the definition by multiplicativity: for $\alpha, \beta \in \mathbb{Z}[\zeta]$ with Norm β not divisible by 3 we define

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\alpha}{\pi_1}\right)_3 \left(\frac{\alpha}{\pi_2}\right)_3 \cdots \left(\frac{\alpha}{\pi_k}\right)_3,$$

where $\pi_i \in \mathbb{Z}[\zeta]$ is prime and $\beta = \pi_1\pi_2\cdots\pi_k$.

Other important properties of the cubic residue symbol are its multiplicativity (in the top argument) and periodicity (in the top argument modulo the bottom argument).

An element $\alpha \in \mathbb{Z}[\zeta]$ is *primary* if and only if $\alpha \equiv 2 \bmod 3$. The primary prime elements of $\mathbb{Z}[\zeta]$ are precisely the positive rational primes $q \equiv 2 \bmod 3$ and the elements $\pi = a + b\zeta$ with $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$ for which Norm $\pi = a^2 - ab + b^2 = p \equiv 1 \bmod 3$ is prime. Among the associates of any $\beta \in \mathbb{Z}[\zeta]$ of norm not divisible by 3 exactly one is primary, and if β is primary it can be written uniquely (up to order) as a product of primary prime elements and a power of the primary unit -1.

The following theorem summarizes the results of the cubic reciprocity law, its supplementary law, and a result on units. For proofs see [21], [2].

Theorem 3.2. *If $\alpha, \beta \in \mathbb{Z}[\zeta]$ are primary elements of norm not divisible by 3 then:*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3.$$

If $\beta \in \mathbb{Z}[\zeta]$ is a primary prime element, $\beta = (3m-1) + b\zeta$, with $b \equiv 0 \bmod 3$ then:

$$\left(\frac{1-\zeta}{\beta}\right)_3 = \zeta^{2m}.$$

If $\pi \in \mathbb{Z}[\zeta]$ is a prime element of norm not equal to 3 then

$$\left(\frac{-1}{\pi}\right)_3 = \left(\frac{1}{\pi}\right)_3 = 1 \quad \textit{and} \quad \left(\frac{\zeta}{\pi}\right)_3 = \begin{cases} 1 & \textit{if} \ \text{Norm } \pi \equiv 1 \bmod 9, \\ \zeta & \textit{if} \ \text{Norm } \pi \equiv 4 \bmod 9, \\ \zeta^2 & \textit{if} \ \text{Norm } \pi \equiv 7 \bmod 9. \end{cases}$$

Explicit primality tests

If, for fixed even h and $k = 1, 2, \ldots$

$$\left(\frac{\alpha_r}{h\cdot 3^k+1}\right)_3 \neq 1, \quad \text{when} \quad 2 \leq k \equiv r \bmod m,$$

we call $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{Z}[\zeta]^*$ a *cubic non-residue cover* for h. We obtain the following analogue of Theorem 3.1; by $\bar{}$ we denote the automorphism of $\mathbb{Q}(\zeta)$ sending ζ to ζ^2.

Theorem 3.3. *If $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{Z}[\zeta]^*$ forms a cubic non-residue cover for h and $3^k > h$ then*

$$N = h\cdot 3^k + 1 \ \textit{is a prime number} \quad \Longleftrightarrow \quad w_{k-1} \equiv \pm 1 \bmod N,$$

where, with $r \equiv k \bmod m$,

$$w_0 = \text{Tr}\left(\frac{\alpha_r}{\bar{\alpha}_r}\right)^{\frac{h}{2}} \quad \textit{and} \quad w_{j+1} = w_j(w_j^2 - 3), \quad \textit{for } j \geq 0.$$

The same result holds for the family $h\cdot 3^k - 1$. So we see that we find an explicit primality criterion for these families, if we can solve the following problem.

Problem 3.4. Given an even positive integer h not divisible by 3, find a finite set $\mathcal{S}_h^+ = \{(r, m, \alpha)_j : j = 1, \ldots, t\}$ of tuples (r, m, α) consisting of residue classes $r \bmod m$ that form a finite covering system such that for integers k with $3^k > h$ and $k \equiv r \bmod m$ it holds that

$$\left(\frac{\alpha}{h\cdot 3^k + 1}\right)_3 \neq 1.$$

Similarly, for the set $\mathcal{S}_h^-$, we require

$$\left(\frac{\alpha}{h\cdot 3^k - 1}\right)_3 \neq 1.$$

Here is the Magma code with which we solved the problem for all $h < 10^5$ (except for h of the form $h = 27^s - 1$ for which there are no solutions). We give the case $h \cdot 3^k - 1$ below; for the similar function *plusfind* replace the appropriate $-$ sign by a $+$ in the computation of N.

```
minfind := function(h, bound, PX)
  i := 0;
  K := [1];
  repeat
    i +:= 1;
    N := h*3^i - 1;
    _, I := get(N, PX);
    if IsEmpty(I) then return 0; end if;
    J := cut(I);
    K := Sort([ Lcm(k,j) : k in K, j in J | Lcm(k,j) lt bound ]);
    if IsEmpty(K) then
      return 0;
    else
      K := cut(K);
    end if;
  until i in K;
  return i;
end function;
```

The function *minfind* calls a function *get*, where most of the work is done, as well as the function *cut* that simply removes from a sequence of positive integers *I* all entries that are divisible by an entry with smaller index.

The main function *get* (which will work both for *minfind* and for *plusfind*) does the following. For given N (which will be of the form $h \cdot 3^k \pm 1$), a list *P* of primes p is found for which the cubic residue symbol for p over N is not equal to 1; the smallest e such that p divides $3^e - 1$ is also stored. For each prime p a prime $\pi \in \mathbb{Z}[\zeta]$ lying over p is found and put in *PX*, that will then consist of a sequence of sequences of prime divisors π of $3^i - 1$ in position i. The function ***cubicsymbol*** is a straightforward implementation of the cubic residue symbol (code not reproduced here).

```
get := function(N, PX)
  S := [ Parent(ζ) | ];
  OS := [ ];
  for i in [1..#PX] do
    if IsEmpty(PX[i]) then
      continue;
    end if;
    for x in PX[i] do
      if cubicsymbol(x[1], x[2], N, 0) ne 1 then
        if x notin S then
          Append(~S, x);
          Append(~OS, i);
        end if;
      end if;
    end for;
  end for;
  return S, OS;
end function;
```

In *minfind* (or *plusfind*) the information from ***get*** is recorded for $N = h \cdot 3^i - 1$ for $i = 1, 2, \ldots$ until a value $i = k$ is reached with the property that for all i with $1 \leq i \leq k$ at least one of the prime divisors of $3^k - 1$ has cubic symbol not equal to 1. The value for *bound* is an upper bound for the solution that will be found; a small value gives quicker results, but it may be that no solution k less than this value exists, and a retry with larger bound will be necessary.

Example 3.5. We attempt to find an explicit primality test for integers of the form $1900 \cdot 3^k - 1$. To this end we run *minfind* with $h = 1900$, and a bound of 25. This means that we will make use only of prime divisors of $3^e - 1$ for e up to 25 (Magma's Cunningham facility will happily supply such divisors for e up to 400 or more). In *PX* both the inert primes (those that are 2 mod 3) and the primes in $\mathbb{Z}[\zeta]$ lying over rational primes that are 1 mod 3 are collected.

In the first round *minfind* will find in *PX* primes that give cubic symbol not equal to 1 with $N_1 = 1900 \cdot 3^1 - 1 = 5699$. It finds the element $29 + 36\zeta$ of norm 1093 (which divides $3^7 - 1 = 2186$), the element $5 + 9\zeta$ of norm 61 (dividing $3^{10} - 1$), $8 + 9\zeta$ (dividing $3^{12} - 1$), and elements dividing $3^{13} - 1$, $3^{14} - 1$, $3^{15} - 1$, $3^{16} - 1$, $3^{19} - 1$, $3^{20} - 1$, and $3^{22} - 1$. For example

$$\left(\frac{29 + 36\zeta}{5699}\right)_3 = \left(\frac{5 + 9\zeta}{5699}\right)_3 = \zeta, \quad \left(\frac{8 + 9\zeta}{5699}\right)_3 = \zeta^2.$$

The sequence *K* will then consist of the integers 7, 10, 12, 13, 15, 16, 19, 22, indicating that these (and their multiples) will have a chance left to act as covering modulus.

It then turns to $N_2 = 1900 \cdot 3^2 - 1 = 17099$; this time elements dividing $3^e - 1$ with the required cubic symbol are found in *PX* for $e = 3$ and all its multiples, for $e = 10$ (and 20), as well as for $e = 14, 16, 19$, and 22, but *not* for $e = 7$ or $e = 13$. This leaves $10, 12, 14, 15, 16, 19, 21, 22$ as possible primitive solutions in *K*.

However, the possibilities $e = 15$ and $e = 16$ disappear when we consider $N_3 = 1900 \cdot 3^3 - 1$, and the possibility $e = 10$ (as well as 20) vanishes when looking at $N_6 = 1900 \cdot 3^6 - 1$, as does $e = 19$. Then $e = 12$ is not good for N_7 (but $e = 24$ is fine), $e = 21$ disappears with N_9 and $e = 22$ with N_{10}. The remaining possibilities are then $e = 14$ and $e = 24$.

It turns out that they also furnish suitable elements for N_{11}, N_{12}, N_{13} and N_{14}. But at that stage we are finished because we know that among the prime divisors of $3^{14} - 1$ we can find suitable elements for N_i with $1 \le i \le 14$; if such an element works for N_i it will also work for N_{i+14}, etc. In other words, we have completed the cover! Indeed, for every $k \ge 1$ at least one of

$$\left(\frac{-13 - 27\zeta}{1900 \cdot 3^k - 1}\right)_3 \in \{\zeta, \zeta^2\}, \quad \left(\frac{29 + 36\zeta}{1900 \cdot 3^k - 1}\right)_3 \in \{\zeta, \zeta^2\}$$

holds, which gives an explicit test by Theorem 3.3. The first holds for all $k > 0$ except the residue classes 4 mod 7 and 5 mod 14, the other for all $k > 0$ in residue classes $0, 1, 4, 5, 6$ mod 7. To make the test completely explicit we would have to compute the trace of the 950th power of $(-13 - 27\zeta)/(-13 - 27\zeta^2)$ and of $(29{+}36\zeta)/(29{+}36\zeta^2)$. Numerator and denominator of the first w_0 have over 2600 decimal digits, however. Of course w_0 will be reduced modulo N; for example, with $N_{69} = 1585331819829053014166528924521037699$ we find $w_{68} = -1$, hence N_{69} is prime.

Sierpiński's problem revisited

It is not hard to see from cubic reciprocity that the rational primes q stored in *PX* will never satisfy

$$\left(\frac{q}{h \cdot 3^k \pm 1}\right)_3 \in \{\zeta, \zeta^2\};$$

what can happen and would be useful for Theorem 3.3, however, is that the symbol becomes 0, implying that for k in a certain residue class $h \cdot 3^k \pm 1$ will be divisible by q.

This also gives the link with our earlier problem: If we adapt our function *get* in such a way that we look for a special cubic non-residue cover consisting only of elements with cubic symbol equal to 0 (rather than not equal to 1), we would detect values for h with the property that $h \cdot 3^k - 1$ or $h \cdot 3^k + 1$ is always divisible by one of a finite set of primes. Conducting this search in the comparable but easier case (using quadratic reciprocity) for numbers of the form $h \cdot 2^k \pm 1$ for h less than 10^6 immediately yields the known examples of Sierpiński and Riesel numbers ([22, 23, 24]). To test divisibility only, there is no need at all to use quadratic or cubic reciprocity, and the test in ***get*** could simply be replaced by a test of the type **if** *N* **mod** *p* ***eq*** 0 **then** for p running over the relevant set of primes. Up to 10^7, however, no h with this property for $h \cdot 3^k \pm 1$ was found.

This led us to attempt to *construct* a 'small' solution in another way (cf. [41, 40]). Just as before, we will find generalized Sierpiński (or Riesel) numbers when we find a finite covering system $\{a_i \bmod m_i\}$ for the exponents k provided that for each modulus m_i we find a prime p_i such that the order of c modulo p_i is a divisor of m_i (that is, p_i divides $c^{m_i} - 1$). We use a table P such that its i-th element contains the primitive prime divisors of $3^i - 1$. Now we wish to construct a covering system for the exponents, but contrary to the situation in the problem of Erdős we will not insist that the moduli are all distinct; however, we will only be able to use the modulus m_i with multiplicity k if there are k different primes in *P*[*i*]. We just apply the function ***try*** defined before, with a sequence of moduli satisfying these requirements. As we explained, it is easy to find H (as $-N^{-1} \bmod \prod_i p_i$) once we know the cover. Since we are now interested in the *smallest possible* value for H, we want to generate all possible covering systems with the same (multi)set of moduli.

Example 3.6. First let $c = 2$ again, the case of Sierpiński numbers. For a very small covering modulus it may be possible to enumerate all covering systems; here is a simple way to do it in Magma.

```
>   S := [ 2,3,4,9,12,18,36 ]; CS := [ ];
>   K := CartesianProduct([ Integers(i) : i in S ]);
>   for x in K do
>     C := [ [ Integers() ! x[i], S[i] ]: i in [1..#S] ]; > if check(C) then
>       Append(~CS, C);
>     end if;
>   end for;
```

The function ***check*** returns true if and only if a given system of residue classes forms a cover (which is tested by simply checking every residue).

Out of the $\#K = 1679616$ posibilities, we find 144 different covers with $S = \{m_1, m_2, \ldots, m_7\}$.

We use the intrinsic 'Chinese Remainder Theorem' function CRT to find, for each of the covers found, the unique H with the property that $H \equiv -2^{-x_i} \bmod p_i$ for all residue classes $x_i \bmod m_i$ in the cover, with p_i a primitive divisor of $2^{m_i} - 1$:

```
>   P := [ 3, 7, 5, 73, 13, 19, 109 ];
>   H := CRT([ -Modexp(2, -C[i][1], P[i]) : i in [1..#C] ], P);
```

It turns out that 72 distinct Sierpiński numbers are generated this way, the smallest being 934909, and the largest 202876561.

In the above we made one particular choice, $p_7 = 109$, for a primitive prime divisor of $2^{36} - 1$, where an alternative $p'_7 = 37$ was available. Applying the same call CRT to the same set of covering systems

```
>   P := [ 3, 7, 5, 73, 13, 19, 37 ]
>   H := CRT([ −Modexp(2, −C[i][1], P[i]) : i in [1..#C] ], P);
```

we find 75 Sierpiński numbers (they are all listed in [40]), the smallest this time being 78557, the largest 68496137. Curiously, three numbers appear in both lists: 12151397, 45181667, and 68468753.

For larger covering systems such a complete enumeration will no longer be feasible. To find analogues of the Sierpiński numbers for $h \cdot 3^k + 1$ we had to use a probabilistic approach again.

Example 3.7. Let $c = 3$. Suppose we know that 48 can be used as a covering modulus. We could then use *try* to obtain a cover (or several covers), and combine the information using the Chinese Remainder Theorem as before to construct the number H. We should be careful, however, only to use residue classes $x_i \bmod m_i$ in our covering system for which there exist primitive prime divisors of $3^{m_i} - 1$.

For example, here is a list of the sets of odd primitive prime divisors of $3^m - 1$ for divisors m of 48:

1	2	3	4	6	8	12	16	24	48
$\emptyset$	$\emptyset$	$\{13\}$	$\{5\}$	$\{7\}$	$\{41\}$	$\{73\}$	$\{17, 193\}$	$\{6481\}$	$\{97, 577, 769\}$

This tells us that we cannot use a residue class with modulus 2 in the cover; also, we are allowed 3 different residue classes modulo 48, and 2 modulo 16.

Feeding the sequence [3, 4, 6, 8, 12, 16, 16, 24, 48, 48, 48] to *try* produced as one solution the covering system

$$\begin{array}{rrrrr} 1 \bmod 3, & 2 \bmod 4, & 2 \bmod 6, & 3 \bmod 8, & 0 \bmod 12, \\ 7 \bmod 16, & 15 \bmod 16, & 18 \bmod 24, & 30 \bmod 48, & 6 \bmod 48. \end{array}$$

Now

```
>   P := [ 13, 5, 7, 41, 73, 17, 193, 6481, 97, 577 ];
>   H := CRT([ −Modexp(3, −C[i][1], P[i]) : i in [1..#C] ], P);
```

produces the solution $H = 41552862226126268$.

Note that a different choice for the two primes of order 48 produces a different answer, and so does a change in the order in which 17 and 193 are listed.

The smallest number H that we found in our experiments with covering modulus up to 250 with the property that $H \cdot 3^k + 1$ is composite for all $k \geq 1$ is the number 125050976086, which occurs for the covering system

$$\begin{array}{lllll} 2 \bmod 3, & 2 \bmod 4, & 3 \bmod 6, & 0 \bmod 8, & 7 \bmod 9, \\ 4 \bmod 16, & 12 \bmod 16, & 1 \bmod 18, & 13 \bmod 18, & \end{array}$$

with P equal to [13, 5, 7, 41, 757, 17, 193, 19, 37].

Again, a generalized Sierpiński number furnishes an associated generalized Riesel number for $h \cdot 3^k - 1$.

4 The totient function

In this section we consider various questions about the image of ϕ, Euler's totient function. By definition, $\phi(n) = \#\{x : \ 1 \leq x \leq n \mid \gcd(x, n) = 1\}$. Obviously, $\phi(p^k) = (p-1) \cdot p^{k-1}$ for any prime p and every $k \geq 1$. Also, $\phi(s \cdot t) = \phi(s) \cdot \phi(t)$ if $\gcd(s, t) = 1$. It follows immediately that $\phi(n)$ is even when $n > 2$, and since $\phi(1) = \phi(2) = 1$ no odd $m > 1$ is in the image of ϕ. But there are also even m that are not in the image of ϕ; these are called non-totients. The smallest non-totient is $m = 14$. There also exist integers divisible by 4 that are non-totients; the smallest is $4 \cdot 17$. In fact (cf. [30]), for every $\alpha \geq 1$ there exists an odd h such that $2^\alpha \cdot h$ is a non-totient; the smallest such h we denote by h_α. There is a connection with Sierpiński numbers, as follows. If $h \cdot 2^n + 1$, for some $n \geq 1$, is a prime number, then $\phi(h \cdot 2^n + 1) = 2^n \cdot h$, and, more generally, $\phi(2^r \cdot (h \cdot 2^n + 1)) = 2^{r-1} \cdot 2^n \cdot h$, so $\phi(x) = 2^k \cdot h$ has solutions for any $k \geq n$. If $h = 2^s + 1$ and $2^s + 1$ is a prime number, then $\phi(x) = 2^s \cdot h$ has solution $x = h^2$, and more generally $2^r \cdot h^2$ is a solution to $\phi(x) = 2^{r-1} \cdot 2^s \cdot h$, so $\phi(x) = 2^k \cdot h$ has solutions for all $k \geq s$. But if h is an odd prime, h is not of the form $2^s + 1$ and $h \cdot 2^n + 1$ is composite for any $n \geq 1$, then there will exist no k for which $\phi(x) = 2^k \cdot h$. Thus any Sierpiński number h that is prime but not a Fermat prime has the property that $\phi(x) = 2^k \cdot h$ has no solution for any $k \geq 0$. The smallest known prime Sierpiński number is $h = 271129$. So, neither h nor any power of 2 times h is in the image of ϕ for $h = 271129$, and $h_\alpha \leq 271129$ for every $\alpha \geq 1$.

The inverse of the Euler ϕ function

We will now describe a function, available in Magma as EulerPhiInverse, that determines $\phi^{-1}(m)$ for any $m \geq 1$.

When solving the equation $\phi(x) = m$ we first note that there will be no solution for odd m exceeding 1. For even m we store the powers of 2 dividing m in an indexed set (for efficient look-up).

```
inv := function(m)
  mfact := Factorization(m);
  if IsEven(m) then
    twopows := {@ 2^i : i in [0..mfact[1][2]] @};
  else
    if m gt 1 then return [ ]; end if;
```

```
        twopows := {@ 1 @};
    end if;
```

Any odd prime p dividing x must have the property that $p-1$ divides m and that p^2 can only divide x for such p if p also divides m.

The idea of the algorithm is to build up integers x from primes p for which $\phi(p) = p-1$ divides m. We keep a list of pairs of partially built up integers a and remainder integers $m/\phi(a)$, and have found a solution whenever the remainder becomes 1.

We start by putting the odd primes p such that $m \equiv 0 \bmod p-1$ in *P*; we deal with the prime 2 separately at the end.

```
    D := Divisors(mfact);
    P := [ ];
    for d in D do
      if d eq 1 then continue; end if;
      if IsPrime(d+1) then
        Append(~P, d+1);
      end if;
    end for;
```

In *S* we will store pairs (a, b) such that a is odd (kept in factored form) and $\phi(a) = m/b$ with b even or 1; clearly, when $b = 1$ we have found a solution $n = a$ to our equation, and $2 \cdot a$ is another solution. More generally, when $b = 2^k$ is a power of 2 we always have a solution $n = 2 \cdot b \cdot a$.

Initially we put $(1, m)$ in *S*, and then loop through the primes p in *P*, checking for every pair (a, b) already in *S* whether b is divisible by $p-1$; if so, we append a pair $(a \cdot p, b/(p-1))$ to *S*, and also a pair $(a \cdot p^2, b/((p-1) \cdot p))$ if p divides b, and so on for higher powers of p, except when the second value is odd and greater than 1.

In this algorithm it is most restrictive, and hence efficient, to treat the primes in *P* in *descending* order.

```
    S := [ <SeqFact([ ]), m> ];
    for p in Reverse(P) do
      for s in S do
        if s[2] eq 1 then continue; end if;
        k := 1;
        d, mmod := Quotrem(s[2], p-1);
        while mmod eq 0 do
          if IsEven(d) or d eq 1 then
            Append(~S, <SeqFact([<p, k>])*s[1], d>);
          end if;
          k +:= 1;
          d, mmod := Quotrem(d, p);
        end while;
      end for;
```

```
  end for;
```

The last prime $p = 2$ is dealt with in a special way, since at the end of this loop only those pairs (a, b) in *S* will be of use for which b is a power of 2. Every such pair contributes a solution as we indicated above, or even two in case $b = 1$. On the other hand it is also easy to see that we find all possible solutions this way, and hence all that remains is to assemble these solutions, and to sort and return them.

```
  R := {};
  for s in S do
    j := Index(twopows, s[2]);
    if j gt 0 then
      Include(~R, SeqFact([<2, j>] cat s[1]));
      if j eq 1 then
        Include(~R, s[1]);
      end if;
    end if;
  end for;
  return Sort([ Facint(nf) : nf in R]);
end function;
```

Example 4.1. Looking at the equation $\phi(n) = m = 1012$, we find first that *P*=[2, 3, 5, 23, 47, 1013], and in the loop for $p = 1013$ only the pair $(1013, 1)$ is added to the list *S* consisting initially of $(1, 1012)$. For *p*=47 we see that the second value of the pair $(1, 1012)$ is divisible by $\phi(47) = 46$, and we add a pair $(47, 22)$ to *S*. For $p = 23$ we add a pair $(23, 46)$ and a pair $(23^2, 2)$, and also a pair $(23{\cdot}47, 1)$ because $(47, 22)$ was in *S*. For $p = 5$ nothing happens, but with $p = 3$ we add $(3, 506)$ and also $(3{\cdot}23^2, 1)$ because $(23^2, 2)$ was in *S*. That means that when we start considering the last prime $p = 2$ in *P*, *S* contains the useful pairs $(1013, 1)$, $(47, 22)$, $(23, 46)$, $(23^2, 2)$, $(23 \cdot 47, 1)$, $(3, 506)$, and $(3 \cdot 23^2, 1)$. This furnishes the solutions 1013, and $1081 = 23{\cdot}47$, and $1587 = 3{\cdot}23^2$, as well as twice these numbers. Finally, the pair $(23^2, 2)$ implies that also $2116 = 2^2 \cdot 23^2$ is a solution. Thus $\phi^{-1}(12) = \{1013, 1081, 1587, 2026, 2116, 2162, 3174\}$.

Carmichael's conjecture

One of the striking properties of the inverse Euler-ϕ function is that when n ranges over the natural numbers, the size $\#\phi^{-1}(n)$ of the set of inverse images of n seems to assume every possible natural number — except 1. *Carmichael's conjecture* states that for no n can there be exactly one solution to the equation $\phi(x) = n$. Carmichael thought he had a proof [11], but it was erroneous; it was replaced by an argument showing that any solution would have to be very large [12], an argument that was refined later [25, 37] to show that any solution will have at least 10^7 decimal digits (see also [34]).

We recorded #EulerPhiInverse(*m*) while executing a simple loop over even m. The results given here concerned the computations for the 327 million even integers up to 654000000. The table lists for some values of k how many m in the range given were found such that #EulerPhiInverse(m) equals k, as well as the smallest n for which #EulerPhiInverse(m) equals k.

0	234369438	14
1	0	–
2	34885680	10
5	3936195	8
10	1964797	24
50	74409	1680
100	18425	34272
500	603	2363904
1000	129	1360800
2500	12	36408960
5000	3	107520000
63255	1	638668800

The last line in the table shows the maximum size that was found: there are 63255 integers x with $\phi(x) = 638668800$.

The smallest value k for which no m was encountered with $\#\phi^{-1}(m) = k$ was $k = 4077$. It is an open conjecture that every $k > 1$ will occur eventually.

Erdős proved [17] that if there exists an integer m for which $\#\phi^{-1}(m) = k$, then there exist infinitely many such m. This was done by a fairly complicated analytic argument, showing that there are very many primes p such that $\#\phi^{-1}((p-1)m) = \#\phi^{-1}(m) = k$.

Iteration of $\phi \circ \sigma$

Another conjecture about ϕ concerns the iteration of the composite $\phi \circ \sigma$ of ϕ and the divisor-σ function, which assigns to n the sum of its divisors $\sigma(n) = \sum_{d|n} d$. The conjecture, formulated by Poulet in [35] as 'loi empirique', states that this function will ultimately cycle for every input n. Meade and Nicol [28] found that for the starting value $n_1 = 455536928 = 2^5 \cdot 7^6 \cdot 11^2$ no cycle had occurred yet when they had computed iterates of $\phi \circ \sigma$ up to 50 digits long, and they state that 'In independent studies Sid Graham has observed that this appears to be the smallest number which does not cycle'. One part of this claim we can prove incorrect here: If the function does not cycle for n_1, this is certainly not the smallest such starting value. The reason is that the sequence of iterates for n_1 merges with the sequence for the starting value $n_0 = 254731536 = 2^4 \cdot 3^2 \cdot 17^2 \cdot 6121$ after a few steps. As a matter of fact, there are almost 400 starting values smaller than n_1 leading to the same sequence, and n_0 is the smallest. After 29781 iterations on n_0 we reached the 179 digit number

$$2^{106} \cdot 3^{70} \cdot 5^{40} \cdot 7^{18} \cdot 11^{11} \cdot 13^4 \cdot 17^2 \cdot 19^3 \cdot 23^3 \cdot 31^2 \cdot 37 \cdot 41 \cdot 59 \cdot \\ 61^2 \cdot 67 \cdot 229 \cdot 271 \cdot 347 \cdot 733 \cdot 5569 \cdot 18211 \cdot 33791 \cdot 83151337.$$

We stopped at this point for no particular reason.

Here are some more statistics about what happens up to starting value $255 \cdot 10^6$. All but one of the sequences, the one starting with n_0, end in one of 46 different cycles. Of these cycles, 20 are of length 1, namely (listing the number of occurrences in parentheses):

1	(1),	$712800 = 2^5 \cdot 3^4 \cdot 5^2 \cdot 11$	(7741)
2	(3),	$1140480 = 2^8 \cdot 3^4 \cdot 5 \cdot 11$	(44858)
$8 = 2^3$	(6),	$1190400 = 2^9 \cdot 3 \cdot 5^2 \cdot 31$	(1833)
$12 = 2^2 \cdot 3$	(7),	$3345408 = 2^{10} \cdot 3^3 \cdot 11^2$	(73649)
$128 = 2^7$	(37),	$3571200 = 2^9 \cdot 3^2 \cdot 5^2 \cdot 31$	(128258)
$240 = 2^4 \cdot 3 \cdot 5$	(43),	$5702400 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 11$	(1149102)
$720 = 2^4 \cdot 3^2 \cdot 5$	(151),	$14859936 = 2^5 \cdot 3^6 \cdot 7^2 \cdot 13$	(48306)
$6912 = 2^8 \cdot 3^3$	(1919),	$29719872 = 2^6 \cdot 3^6 \cdot 7^2 \cdot 13$	(44113)
$32768 = 2^{15}$	(160),	$50319360 = 2^{12} \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$	(1135829)
$142560 = 2^5 \cdot 3^4 \cdot 5 \cdot 11$	(1374),	$118879488 = 2^8 \cdot 3^6 \cdot 7^2 \cdot 13$	(290673)

We found 11 cycles of length 2, 5 cycles of length 3, 3 cycles of length 4 and 2 cycles of length 6, as well as single cycles of lengths 9, 11, 12, 15, and 18. The following table lists some of them (again, the number of occurrences in brackets), cf. [5].

length 2*:*

$[4, 6]$ (7),
$[3852635996160, 4702924800000]$ (123),

length 3*:*

$[16, 30, 24]$ (35),
$[272160, 290304, 290400]$ (413972),

length 4*:*

$[2142720000, 2935296000, 3311642880, 3185049600]$ (16),

length 9*:*

$[113218560, 124895232, 163296000, 181149696, 170698752,$
$125798400, 116121600, 139708800, 136857600]$ (7682341),

length 15*:*

$[40255488, 48384000, 43130880, 41912640, 47029248,$
$70253568, 91998720, 82944000, 83825280, 71663616,$
$52428800, 79221120, 70778880, 57600000, 42456960]$ (128378949),

length 18*:*

$[150493593600, 152374763520, 202491394560, 167215104000,$
$219847799808, 161864220672, 247328774784, 191102976000,$
$207622711296, 178362777600, 283740364800, 233003796480,$
$221908377600, 204838502400, 214695936000, 237283098624,$
$185794560000, 178886400000]$ (82683195).

It is surprising that so many sequences end in so few cycles. One should not get the impression, however, that it is difficult to find other cycles. Starting values $n = 2^\ell$ for example, frequently lead to new ones. Indeed, for $\ell = 33$ we find a cycle of length 21, and for $\ell = 40$ we find a cycle of length 22. We list a few more values below.

ℓ	*length*	*minimal entry*
33	21	12227604480
41	3	4672651788288000
45	8	140005324800000
52	34	19937391280128000
54	9	1401456438084102782976000000
79	5	6634509269055173050761216000
88	56	42313405772261648007954432000
89	23	56221811109731562946560000

For larger values of ℓ the sequence of iterates seems to keep growing for a long time. All of this hardly provides evidence for or against the conjecture that every starting value eventually leads to a cycle.

Fixed points

A related question concerns fixed points under $\phi \circ \sigma$: solutions in positive integers to $\phi \circ \sigma(n) = n$. According to Guy (Problem B42 in [20]) Selfridge, Hoffman and Schroeppel found all but the final value $2^8 \cdot 3^6 \cdot 7^2 \cdot 13$ mentioned in the table of the previous section, and in addition

$$\begin{aligned} 2147483648 &= 2^{31} \\ 4389396480 &= 2^{13} \cdot 3^7 \cdot 5 \cdot 7^2 \\ 21946982400 &= 2^{13} \cdot 3^7 \cdot 5^2 \cdot 7^2 \\ 11681629470720 &= 2^{21} \cdot 3^3 \cdot 5 \cdot 11^3 \cdot 31 \\ 58408147353600 &= 2^{21} \cdot 3^3 \cdot 5^2 \cdot 11^3 \cdot 31 \end{aligned}$$

We tried the following code in Magma to generate some more solutions, using various values for A to produce a list of primes P and maximal exponents E:

```
>   A := 35;
>   P := [ n : n in [2..A] | IsPrime(n) ];
>   E := [ Floor(A/p) : p in P ];
>   C := CartesianProduct([ [ e..0 by −1] : e in E ]);
>   for c in C do
>     nfn := SeqFact([ <P[i], c[i]> : i in [1..#P] | c[i] ne 0 ]);
>     if EulerPhi(DivisorSigma(1, nfn)) eq Facint(nfn) then
>       print nfn;
>     end if;
>   end for;
```

Here are some of the 25 new solutions we found (cf. [5]):

$$\begin{aligned} 118879488 &= 2^8 \cdot 3^6 \cdot 7^2 \cdot 13 \\ 3889036800 &= 2^9 \cdot 3^4 \cdot 5^2 \cdot 11^2 \cdot 31 \\ 116827283381708390400000 &= 2^{25} \cdot 3^{11} \cdot 5^6 \cdot 7^4 \cdot 13^2 \cdot 31 \\ 1487719960639259421126804111136 \cdot 10^7 &= 2^{35} \cdot 3^{21} \cdot 5^7 \cdot 7^2 \cdot 11^4 \cdot 13^2 \cdot 19 \cdot 23 \end{aligned}$$

5 Class number relations

The final examples concern the art of computing with character relations.

A *character relation* for a finite group G consists of a sequence of integers a_H, one for every subgroup H of G, such that $\sum a_H 1_H^G = 0$, when we sum over all subgroups. Here $\chi = 1_H^G$ is the *permutation character* of the subgroup H, so $\chi(g)$ is the integer counting the number of cosets of H left invariant by the action of g. The number theoretic significance of character relations follows from a theorem of Brauer [9],

$$\#\{ \prod_{H<G} h(N^H)^{a_H} : \ \ \mathrm{Gal}(N/\mathbb{Q}) = G \ \} < \infty,$$

expressing that the class number products with multiplicities according to a character relation for G assume finitely many different rational values when N ranges over all normal number fields with Galois group G. Here $h(N^H)$ is the ideal class number of the ring of integers of the subfield of N fixed by the elements of the subgroup H of G. To prevent trivial cases we will assume that in the character sums (and the related class number products) the sum (and product) ranges over non-conjugate subgroups only.

In Magma the permutation characters for all subgroups of a given permutation group G can be generated, as a matrix with the characters as rows, by this function:

```
permcharmat := function(G)
  nc := #ConjugacyClasses(G);
  subs := Subgroups(G);
  M := Hom(RSpace(Integers(), #subs), RSpace(Integers(), nc));
  return M !
        &cat[ Eltseq(PermutationCharacter(G, s`subgroup)) : s in subs ];
end function;
```

The intrinsic function Subgroups returns a representative for all conjugacy classes of subgroups of a permutation group as a sequence of *records*, one for each class. Each record contains the representative of the class, which can be obtained via the *attribute* 'subgroup', here in the form *s`subgroup*, where *s* is one of the records in the sequence *subs*. Other attributes that can be used on this record are *s`order* for the order of the subgroup and *s`length* for the number of different subgroups that are in the class.

Here is the result for the alternating group on 4 letters:

```
> permcharmat( Alt(4) );
        [12  0  0  0]
        [ 6  2  0  0]
        [ 4  0  1  1]
        [ 3  3  0  0]
        [ 1  1  1  1]
```

The character relations are the non-trivial relations between the rows of this matrix, and they can simply be generated as its kernel:

```
> relations := func< G | Kernel( permcharmat(G) ) >;
> relations( Alt(4) );
        RSpace of degree 5, dimension 2 over Integer Ring
        Echelonized basis:
        ( 1  0 -3 -1  3)
        ( 0  1 -1 -1  1)
```

Thus, for A_4, all character relations can be derived from the basis pair given here. According to Brauer's theorem the class number products corresponding to these relations

$$\frac{h(N)\cdot h(\mathbb{Q})^3}{h(N_4)^3\cdot h(N_3)}, \qquad \frac{h(N_6)\cdot h(\mathbb{Q})}{h(N_4)\cdot h(N_3)}$$

take on finitely many values as N ranges over all Galois extensions of $\mathbb{Q}$ with Galois group A_4. Here we used the notation N_d for the degree d subfield of N invariant under the index d subgroup of A_4; of course $h(N_1) = h(\mathbb{Q}) = 1$ in this notation. In [7], Example 5.3, it is shown that the set of rationals that will occur is included in $\{\frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2\}$.

Arithmetically equivalent fields

The simplest non-trivial character relation occurs when G has a pair H, H' of non-conjugate subgroups with the same permutation character. The corresponding invariant subfields $N^H, N^{H'}$ of the normal field N with Galois group G will then be non-isomorphic but they share many properties: they will have the same zeta-function [32]. Such fields are called *arithmetically equivalent.*

The existence of arithmetically equivalent number fields was shown by Gassmann [18], who exhibited in 1926 two non-conjugate subgroups of the symmetric group on 6 elements (both isomorphic to V_4) with the same permutation character:

```
> G := Sym(6);
> U := sub< G | (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) >;
> V := sub< G | (1,2)(3,4), (1,2)(5,6), (3,4)(5,6) >;
> PermutationCharacter(G, U);
        ( 180, 0, 0, 12, 0, 0, 0, 0, 0, 0, 0 )
```

```
> PermutationCharacter(G, V);
      ( 180, 0, 0, 12, 0, 0, 0, 0, 0, 0, 0 )

> Induction(PrincipalCharacter(U), G) eq PermutationCharacter(G, U);
      true
```

The last line is included here by way of explanation for the notation 1_U^G for the permutation character: it is the character on G induced by the principal character on U. In this case it is easy to see that $1_U^G = 1_V^G$ if one uses the equivalent property that $C \cap U = C \cap V$ for all conjugacy classes C of G; the latter is obvious as conjugacy classes in S_n coincide with cycle types, and U and V are clearly the same in this respect. Since U fixes the points $5, 6$ and V is fix-point free, U and V are non-conjugate in G.

The degree of the equivalent number fields in this case is 180 (being the index of U in G, which equals the first character value). Since S_6 is the generic group for an irreducible polynomial of degree 6, the construction will furnish infinitely many pairs of arithmetically equivalent fields.

To search for examples of small degree n in Magma, one uses a simple double loop over all transitive subgroups G of S_n. Since only subgroups of index n are relevant, we set the parameter OrderEqual on the intrinsic Subgroups equal to $\#G/n$, and search for pairs U, V of subgroups isomorphic to a point stabilizer but not conjugate in S_n:

```
> for n := 1 to 12 do
>   for k := 1 to NumberOfTransitiveGroups(n) do
>     G := TransitiveGroup(n, k);
>     U := Stabilizer(G, 1);
>     χ := PermutationCharacter(G, U);
>     S := Subgroups(G : OrderEqual := Order(G) div n);
>     if exists(i){ i : i in [1..#S] | PermutationCharacter(G, V) eq χ
>                 and IsEmpty(Fix(V)) where V := S[i]`subgroup } then
>       < n, k, Order(G)>;
>     end if;
>   end for;
> end for;
      <7, 5, 168>
      <8, 15, 32>
      <8, 23, 48>
      <11, 5, 660>
      <12, 26, 48>
      <12, 38, 72>
      <12, 49, 96>
      <12, 57, 96>
      <12, 104, 192>
      <12, 124, 240>
```

This computation reproduces part of the table given in [8], see also [26], and proves that there exist precisely 10 different configurations of pairs of arithmetically equivalent fields in degrees up to 12, namely one in degree 7, two in degree 8, one in degree 11, and six in degree 12. This non-trivial computation can only be done efficiently (in a matter of minutes) because of the availability of a database of transitive groups and a fast subgroup algorithm [10].

This computation confirms the theoretical proof of Perlis [31] that no non-trivial character relations exist for permutation groups of degree less than 7.

An arithmetically equivalent family in degree 7

A family of arithmetically equivalent pairs of number fields consists of a parametrized pair of polynomials that generically generate subfields of a Galois extension invariant under the pair of subgroups of a given configuration (as in the previous section). In this section we show how this can be done for the configuration in the smallest possible degree 7.

If we replace the line that produces output in the previous code fragment by

```
>       < n, k, G, U, S[i]`subgroup >;
```

it would output this for the degree 7 case:

```
<7, 5,
Permutation group G acting on a set of cardinality 7
Order = 168 = 2^3 * 3 * 7
    (1, 2, 3, 4, 5, 6, 7)
    (1, 2)(3, 6),
Permutation group U acting on a set of cardinality 7
Order = 24 = 2^3 * 3
    (2, 3)(4, 7)
    (2, 7, 5)(3, 6, 4)
    (3, 7)(5, 6)
    (3, 6)(5, 7),
Permutation group acting on a set of cardinality 7
Order = 24 = 2^3 * 3
    (1, 6)(4, 7)
    (1, 6, 5)(2, 3, 7)
    (2, 4)(3, 7)
    (2, 3)(4, 7)>
```

In [8] it is shown how the two subgroups U, V of the simple group $G \cong \mathrm{GL}_3(\mathbb{F}_2)$ of 168 elements can be related to each other geometrically. If N is Galois with group G and the invariant field N^U is generated by the irreducible degree 7 polynomial f, then V leaves 'collinear' triples of roots of f invariant, when we identify the 7 roots of f with the points of the projective plane over $\mathbb{F}_2$; so N^V is generated by a polynomial of degree 7 having sums of collinear roots of f as its roots.

The following notation will be used for the particular family of arithmetically equivalent fields that will be considered here. For $s, t \in \mathbb{Q}$ let $f_{s,t}$ be defined as

$$x^7 + (-6t+2)x^6 + (8t^2+4t-3)x^5 + (-s-14t^2+6t-2)x^4$$
$$+(s+6t^2-8t^3-4t+2)x^3 + (8t^3+16t^2)x^2 + (8t^3-12t^2)x - 8t^3.$$

If $f_{s,t}$ is irreducible over $\mathbb{Q}$ then the number field obtained by adjoining a root of $f_{s,t}$ to $\mathbb{Q}$ will be denoted by K, and the field defined by $f_{-s,t}$ will be denoted by K'. The Galois closure of K will be denoted by N as usual.

Magma can be used in the proof of the following proposition, cf. [8].

Proposition 5.1. *If $f_{s,t}$ is irreducible in $\mathbb{Q}[x]$, then so is $f_{-s,t}$; the Galois group of $f_{s,t}$ is a subgroup of $\mathrm{GL}_3(\mathbb{F}_2)$, and when it equals $\mathrm{GL}_3(\mathbb{F}_2)$ then K and K' are arithmetically equivalent.*

LaMacchia [27] already showed that the Galois group $\mathrm{Gal}(N/\mathbb{Q})$ of $f_{s,t}$ is generically $\mathrm{GL}_3(\mathbb{F}_2)$. The remarks above imply that we can identify a polynomial generating K' as an irreducible factor g of degree 7 of the polynomial P of degree 35 that has *all* sums of three roots of $f_{s,t}$ as roots. We determine this polynomial here symbolically; for the paper [8] a modular approach was used.

```
>  F<s,t> := FunctionField(Rationals(), 2);
>  Q<x> := PolynomialRing(F);
>  f := x^7 + (-6*t+2)*x^6 + (8*t^2+4*t-3)*x^5 +
>     (-s-14*t^2+6*t-2)*x^4 + (s+6*t^2-8*t^3-4*t+2)*x^3 +
>     (8*t^3+16*t^2)*x^2 + (8*t^3 - 12*t^2)*x - 8*t^3;
```

We determine the polynomial q_1 having as roots all sums of pairs of distinct roots of $f_{s,t}$. For this, observe that the resultant of $f(x-y)$ and $f(y)$ with respect to y is a polynomial in x that consists of the product of all differences of the roots $x-\alpha_i$ of $f(x-y)$ and α_j of f:

$$r = \mathrm{Res}_y(f(x-y), f(y)) = -\prod_{1\le i,j\le 7}(x-\alpha_i-\alpha_j) = -q_1^2\cdot h_2,$$

where h_2 is the monic polynomial that has the sums of two equal roots of f as its root. To work with monic polynomials throughout we replace f by the monic version h_1 of $f(-x)$.

```
>  h1 := (-1)^Degree(f)*Evaluate(f, -x);
>  Y<y> := PolynomialRing(Q);
>  r := Resultant(Evaluate(h1, y-x), Evaluate(f, y));
>  h2 := 2^7*Evaluate(f, x/2);
>  q1 := SquareRoot(r div h2);
```

The resulting polynomial q_1 of degree 21 is

$$q_1 = x^{21} + (-36t+12)x^{20} + \cdots(-147456t^{13} + \cdots - 8s^4t^3 + \cdots - 384t^5).$$

To find P, repeat the resultant trick. Determine the polynomial q having as roots the sums of three roots of f, at least two of them equal, and also q_2, having as roots the sum of one root and twice another root of f:

```
>    q := Resultant(Evaluate(h1, y-x), Evaluate(h2, y));
>    h3 := 3^7*Evaluate(f, x/3);
>    q2 := q div h3;
```

then the polynomial P having sums of three distinct roots of f as its roots is easily obtained:

```
>    R := Resultant(Evaluate(h1, y-x), Evaluate(q1, y));
>    P := Root(R div q2, 3);
```

From this polynomial P of degree 35, which has 2668 non-zero terms, we obtain the desired polynomial g by factorization:

```
>    fP := Factorization(P);
>    g := fP[1][1]; g;
         x^7 + (-18*t + 6)*x^6 + (124*t^2 - 64*t + 6)*x^5 + (-408*t^3 +
          208*t^2 - 4*t - 16)*x^4 + (6*s*t - 6*s + 640*t^4 - 156*t^3 -
          116*t^2 + 84*t - 27)*x^3 + (-36*s*t^2 + 36*s*t - 12*s -
          384*t^5 - 152*t^4 + 120*t^3 + 88*t^2 - 34*t - 6)*x^2 +
          (-s^2 + 48*s*t^3 - 20*s*t^2 - 2*s*t - 2*s - 64*t^5 - 84*t^4 +
          52*t^3 - 8*t^2 - 12*t)*x - 8*s*t^3 - 4*s*t^2 + 384*t^6 +
          80*t^5 - 88*t^4 - 24*t^3
```

The bottlenecks in this computation are the root extraction $P = \sqrt[3]{R/q_2}$ and the factorization of P. The polynomial R has degree 147 and

```
>    &+[ #Terms(Integers(F) ! c) : c in Coefficients(R) ];
         165555
```

non-zero terms.

Finally we show that $f_{-s,t}$ and g generate the same number field. Instead of literally pasting in the definition of $f_{-s,t}$ we obtain it by applying the homomorphism h of $F(s,t)[x]$ sending s to $-s$:

```
>      fh := hom< F -> F | -s, t >;
>      h := hom< Q -> Q | fh, x >;
>      fminus := f@h;
```

When we apply a particular rational transformation to g the result is divisible by *fminus*,

```
>      gnew := Q ! x^7*Evaluate(g, (x-1)*(1+2*t/x));
>      gnew mod fminus;
         0
```

and the proposition follows.

Class number quotients

Arithmetically equivalent number fields have the same zeta-function; the zeta-function encodes a lot of information but it is not true that number fields are characterized (up to isomorphism) by their zeta-function. Equality of zeta-functions for two fields forces many invariants of the fields to be equal, but not necessarily their ideal class numbers. However, the product of class number and *regulator* for arithmetically equivalent fields will be the same.

The first example of number fields with the same zeta-function but different class numbers was published by Perlis and de Smit [39]. It consists of a pair of arithmetically equivalent fields in degree 8 of the form $\mathbb{Q}(\sqrt[8]{a}), \mathbb{Q}(\sqrt[8]{16a})$.

Work by de Smit has produced bounds on the possible class number quotients that appear in the finite set $h(N^H)/h(N^{H'})$ for a fixed triple (G, H, H') that produces arithmetically equivalent number fields N^H and $N^{H'}$ with $G = \mathrm{Gal}(N/\mathbb{Q})$ of small degree $[G : H]$. These bound are fairly tight in the sense that most remaining quotients do occur. For our example in degree 7 the bounds imply that the set is contained in $\{1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}\}$ and their reciprocals, where $\frac{1}{8}$ would only be possible for a totally real field N (the only other possibility in this configuration is that N has precisely 2 pairs of complex embeddings).

To generate examples the following code could be used. It is useful in practice to search for examples with relatively small discriminant only. Continuing our previous examples with $F = \mathbb{Q}(s, t)$ and $Q = F[x]$

```
>   U<u> := PolynomialRing(Rationals());
>   evalst := func< j, k | hom< Q → U | C, u>
>         where C is hom< F → Rationals() | j, k > >;
```

the function *evalst*$(j,\ k)$ can, for rational values of j, k, be applied to $f_{s,t}$ to cast it into an element of $U = \mathbb{Q}[u]$ by evaluating $s = j$ and $t = k$. Here we use this for some selected values for j and k (obtained from a search):

```
>   for p in [ [1,2], [7,1], [6,−7], [5,4], [1,4], [19,5] ] do
>     j, k := Explode(p);
>     N1 := NumberField( evalst(j,k)(f) );
>     fD := Factorization(Discriminant(Integers(N1)));
>     h1 := ClassNumber(N1: Bound := 300);
>     N2 := NumberField( evalst(−j,k)(f) );
>     h2 := ClassNumber(N2: Bound := 300);
>     print <p, Min([ h1/h2, h2/h1 ]), fD, Signature(N1)>;
>   end for;
      <[ 1, 2 ], 1, [ <27277, 2> ], 3>
      <[ 7, 1 ], 1/2, [ <222107, 2> ], 3>
      <[ 6, -7 ], 1/4, [ <2, 4>, <13, 2>, <1728655121887, 2> ], 3>
      <[ 5, 4 ], 1, [ <8488225021, 2> ], 7>
      <[ 1, 4 ], 1/2, [ <3347, 2>, <2602463, 2> ], 7>
      <[ 19, 5 ], 1/4, [ <270982714837, 2> ], 7>
```

The ideal class numbers for the pair of arithmetically equivalent number fields N_1 and N_2 are calculated, and their quotient is displayed here, together with the field discriminant (in factored form) and the number of real embeddings. The bound of 300, given as a parameter here, speeds up the computation (it puts a bound on the norms of the ideals used as generators for ideal classes), but some additional work is required to obtained guaranteed results. We did not find an example where the quotient equals $\frac{1}{8}$ (or 8).

References

1. R. Baillie, G. Cormack, H. C. Williams, *The problem of Sierpiński concerning* $k \cdot 2^n + 1$, Math. Comp. **37** 1981, 229–231.
2. Bruce C. Berndt, Ronald J. Evans, Kenneth S. Williams, *Gauss and Jacobi sums*, Canad. Math. Soc. series of monographs and advanced texts **21**, New York: John Wiley and Sons, 1997.
3. Wieb Bosma, *Explicit primality criteria for* $h \cdot 2^k \pm 1$, Math. Comp. **61** 1993, 97–109.
4. Wieb Bosma, *Cubic reciprocity and explicit primality tests for* $h \cdot 3^k \pm 1$, in: Alf van der Poorten, Andreas Stein (eds.), *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun. **41**, Providence: Amer. Math. Soc. 2004, 77–89.
5. Wieb Bosma, *Some computational experiments in elementary number theory*, report **05-02** Mathematical Institute, Radboud University Nijmegen, 2005.
6. Wieb Bosma, John Cannon, Catherine Playoust, *The Magma Algebra System I: The User Language* J. Symbolic Computation **24** (1997), 235–265.
7. Wieb Bosma, Bart de Smit, *Class number relations from a computational point of view*, J. Symbolic Computation **31** (2001), 97–112.
8. Wieb Bosma, Bart de Smit, *On arithmetically equivalent number fields of small degree*, in: C. Fieker, D. R. Kohel (eds.), *Algorithmic Number Theory Symposium, Sydney, 2002*, Lecture Notes in Computer Science **2369**, Berlin, Heidelberg: Springer, 2002, pp. 67–79.
9. R. Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachrichten **4** (1951), 158–174.
10. J. J. Cannon, D. F. Holt, *Computing maximal subgroups of a finite group*, J. Symbolic Comput. **37** (2004), 589–609.
11. R. D. Carmichael, *On Euler's ϕ-function*, Bull. Amer. Math. Soc. **13** 1907, 241–243. Errata: Bull. Amer. Math. Soc. **54** 1948, 1192.
12. R. D. Carmichael, *Note on Euler's ϕ-function*, Bull. Amer. Math. Soc. **28** 1922, 109–110. Errata: Bull. Amer. Math. Soc. **55** 1949, 212.
13. S. L. G. Choi, *Covering the set of integers by congruence classes of distinct moduli*, Math. Comp. **25** 1971, 885–895.
14. R.F. Churchhouse, *Covering sets and systems of congruences*, pp. 20–36 in: R.F. Churchhouse, J.-C. Herz (eds.), *Computers in mathematical research*, Amsterdam: North-Holland, 1968.
15. D. W. Erbach, J. Fischer, J. McKay, *Polynomials with* PSL(2, 7) *as Galois group*, J. Number Theory **11** (1979), 69–75.

16. Paul Erdős, *Some of my favorite problems and results*, pp. 47–67 in: Ronald L. Graham, Jaroslav Nešetřil (eds.), *The Mathematics of Paul Erdős I*, Berlin: Springer, 1997.
17. Paul Erdős, *Some remarks on Euler's ϕ function*, Acta Arith. **4** 1958, 10–19.
18. F. Gassmann, *Bemerkungen zu der vorstehenden Arbeit von Hurwitz ('Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe')*, Math. Z. **25** (1926), 124–143.
19. Andrew Granville, K. Soundararajan, *A binary additive problem of Erdős and the order of* $2 \bmod p^2$, Ramanujan J. **2** 1998, 283–298.
20. Richard K. Guy, *Unsolved problems in number theory*, Unsolved problems in intuitive mathematics **I**, New York: Springer 1994 (2nd edition).
21. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Graduate texts in mathematics **84**, New York: Springer, 1982.
22. G. Jaeschke, *On the smallest k such that all $k \cdot 2^N + 1$ are composite*, Math. Comp. **40** 1983, 381–384. Errata: Math. Comp. **45** 1985, 637.
23. Wilfrid Keller, *Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$*, Math. Comp. **41** 1983, 661–673.
24. Wilfrid Keller, *The least prime of the form $k \cdot 2^n + 1$*, Abstracts Amer. Math. Soc. **9** 1988, 417–418.
25. V. L. Klee, Jr., *On a conjecture of Carmichael*, Bull. Amer. Math. Soc. **53** 1947, 1183–1186.
26. N. Klingen, *Arithmetical similarities*, Oxford: Oxford University Press, 1998.
27. Samuel E. LaMacchia, *Polynomials with Galois group* $\mathrm{PSL}(2,7)$, Comm. Algebra **8** (1980), 983–992.
28. Douglas B. Meade, Charles A. Nicol, *Maple tools for use in conjecture testing and iteration mappings in number theory*, IMI Research Report 1993:06 (Department of Mathematics, University of South Carolina), 1993.
29. Ryozo Morikawa, *Some examples of covering sets*, Bull. Fac. Liberal Arts, Nagasaki Univ. **21** 1981, 1–4.
30. Oystein Ore, J. L. Selfridge, P. T. Bateman, *Euler's function*: Problem 4995 and its solution, Amer. Math. Monthly **70** 1963, 101–102.
31. R. Perlis, *On the equation $\zeta_K(s) = \zeta_{K'}(s)$* J. Number Theory **9** (1977), 342–360.
32. R. Perlis, *On the class numbers of arithmetically equivalent fields*, J. Number Theory **10** (1978), 458–509.
33. A. de Polignac, *Recherches nouvelles sur les nombres premiers*, C. R. Acad. Sci. Paris Math. **29** 1849, 397–401; 738–739.
34. Carl Pomerance, *On Carmichael's conjecture*, Proc. Amer. Math. Soc. **43** 1974, 297–298.
35. P. Poulet, *Nouvelles suites arithmétiques*, Sphinx **2** (1932), 53–54.
36. H. Riesel, *Några stora primtal*, Elementa **39** 1956, 258–260.
37. Aaron Schlafly, Stan Wagon, *Carmichael's Conjecture on the Euler function is valid below* $10^{10000000}$, Math. Comp. **63** 1994, 415–419.
38. W. Sierpiński, *Sur un problème concernant les nombres $k \times 2^n + 1$*, Elemente der Mathematik **15** (1960), 63–74.
39. Bart de Smit, Robert Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. **31** (1994), 213–215.
40. R. G. Stanton, *Further results on covering integers of the form $1 + k \cdot 2^n$ by primes*, pp. 107–114 in: Kevin L. McAvaney (ed.), *Combinatorial Mathematics VIII*, Lecture Notes in Mathematics **884**, Berlin: Springer, 1981.

41. R. G. Stanton, H. C. Williams, *Computation of some number-theoretic coverings* pp. 8–13 in: Kevin L. McAvaney (ed.), *Combinatorial Mathematics VIII*, Lecture Notes in Mathematics **884**, Berlin: Springer, 1981.
42. `http://www.prothsearch.net/sierp.html`
43. `http://www.prothsearch.net/rieselprob.html`