# REDUNDANT TRINOMIALS FOR FINITE FIELDS OF CHARACTERISTIC 2

CHRISTOPHE DOCHE

Abstract. In this paper we introduce so-called *redundant trinomials* to represent elements of finite fields of characteristic 2. The concept is in fact similar to *almost irreducible trinomials* introduced by Brent and Zimmermann in the context of random numbers generators in [BZ 2003]. See also [BZ]. In fact, Blake *et al.* [BGL 1994, BGL 1996] and Tromp *et al.* [TZZ 1997] explored also similar ideas some years ago. However redundant trinomials have been discovered independently and this paper develops applications to cryptography, especially based on elliptic curves. After recalling well–known techniques to perform efficient arithmetic in extensions of $\mathbb{F}_2$, we describe redundant trinomial bases and discuss how to implement them efficiently. They are well suited to build $\mathbb{F}_{2^n}$ when no irreducible trinomial of degree $n$ exists. Depending on $n \in [2, 10,000]$ tests with `NTL` show that improvements for squaring and exponentiation are respectively up to 45% and 25%. More attention is given to relevant extension degrees for doing elliptic and hyperelliptic curve cryptography. For this range, a scalar multiplication can be speeded up by a factor up to 15%.

## 1. Introduction

There are mainly two types of bases to compute in finite fields of characteristic 2, namely polynomial and normal bases. It is well known that there is a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for every extension degree $n$. However only a certain category of normal bases, namely optimal normal basis of type I or II can be used in practice. Those bases are quite rare. Considering extension fields of degree up to $10,000$, only 17.07% of them have an optimal normal basis.

For every extension degree, there is a polynomial basis as well. Following an idea of Schroeppel [SOO 1995], sparse irreducible polynomials are commonly used to perform arithmetic in extension fields of $\mathbb{F}_2$ since they provide a fast modular reduction. As a polynomial with an even number of terms is always divisible by $x+1$, we turn our attention to so-called *trinomials*. When no such irreducible polynomial exists, one can always find an irreducible *pentanomial*, at least for extension degrees up to $10,000$. In this range this situation occurs quite often. In fact one has to choose an irreducible pentanomial in about 50% of the cases (precisely 4853 out of 9999 [Ser 1998]).

Next Section describes in more detail efficient algorithms to perform reduction, addition, multiplication, and inversion in $\mathbb{F}_{2^n}/\mathbb{F}_2$.

*Date*: on February 29, 2004.

*Key words and phrases.* Finite fields arithmetic, Elliptic curve cryptography.

## 2. Finite Field Arithmetic

An element of $\mathbb{F}_{2^n} \sim \mathbb{F}_2[x]/\big(\mu(x)\big)$ is uniquely represented as a polynomial $f$ of degree less than $n$ with coefficients in $\mathbb{F}_2$. If $f$ is a polynomial such that $\deg f \geqslant n$ one first reduces $f$ modulo the irreducible polynomial $\mu$. The usual way to get this reduction is to compute the remainder of the Euclidean division of $f$ by $\mu$. When $\mu$ is sparse there is dedicated algorithm which is much faster.

**Algorithm 1.** Division by a sparse polynomial

Input: Two polynomials $\mu(x)$ and $f(x)$ with coefficients in a commutative ring, where $\mu(x)$ is the sparse polynomial $x^n + \sum_{i=1}^{t} a_i x^{b_i}$ with $b_i < b_{i+1}$.
Output: The polynomials $u$ and $v$ such that $f = u\mu + v$ with $\deg v < n$.

1. $v \leftarrow f$, $u \leftarrow 0$
2. **while** $\deg(v) \geqslant n$ **do**
3. $\quad k \leftarrow \max(n, \deg v - n + b_t + 1)$
4. $\quad$ write $v(x) = u_1(x)x^k + w(x)$
5. $\quad v(x) \leftarrow w(x) - u_1(x)\big(\mu(x) - x^n\big)x^{k-n}$
6. $\quad u(x) \leftarrow u_1(x)x^{k-n} + u(x)$
7. **return** $(u, v)$

**Remarks.**

- *If* $\deg f = m$ *then Algorithm 1 needs at most* $2(t-1)(m-n+1)$ *additions to compute* $u$ *and* $v$ *such that* $f = u\mu + v$. *In this case the number of loops is at most* $\lceil (m-n+1)/(n-b_t-1) \rceil$. *If* $m \leqslant 2n-2$, *as it is the case when performing arithmetic modulo* $\mu$, *then the number of loops is at most equal to* 2 *whatever the value of* $b_t$, *as long as* $1 \leqslant b_t \leqslant n/2$.
- *To avoid computing the quotient* $u$ *when it is not required, simply discard line 6. of Algorithm 1.*

Concerning operations, additions are performed at a word level and correspond to xor. Computing a squaring only costs a reduction modulo $f$. Indeed if $f(x) = \sum a_i x^i$ then $f^2(x) = \sum a_i x^{2i}$. Multiplications are also performed at a word level, but processors do not provide single precision multiplication for polynomials. Nevertheless it is possible to emulate it doing xor and shifts. One can also store all the possible single precision products and find the global result by table look–up. This method is fast but for 32–bit words the number of precomputed values is far too big. A tradeoff consists in precomputing a smaller number of values and obtain the final result with Karatsuba's method. Typically two 32–bit polynomials can be multiplied with 9 precomputed multiplications of 8–bit block polynomials [GG 1996].
Once the single precision multiplication is defined, different multiplication methods can be applied depending on the degree of the polynomials. In [GN] the crossover between the schoolbook multiplication and Karatsuba's method is reported to be equal to 576. Other more sophisticated techniques like the F.F.T. or Cantor's multiplication [GG 1996] based on evaluation/interpolation methods can be used

for larger degrees. For example, the crossover between Karatsuba's method and Cantor's multiplication is equal to 35840 in [GN].
There are usually two different ways to compute the inverse of an element of $\mathbb{F}_{2^n}$. The first one is to compute an extended Euclidean gcd. The second one takes advantage of the group structure of $\mathbb{F}_{2^n}^\times$.

**Algorithm 2.** Inverse of an element of $\mathbb{F}_{2^n}^\times$ using extended Euclidean gcd

INPUT: An irreducible polynomial $\mu(x) \in \mathbb{F}_2[x]$ of degree $n$ and a non-zero polynomial $f(x) \in \mathbb{F}_2[x]$ such that $\deg f < n$.
OUTPUT: The polynomial $U(x) \in \mathbb{F}_2[x]$ such that $fU \equiv 1 \pmod{\mu}$.

1. $U \leftarrow 1$, $V \leftarrow 0$, $C \leftarrow \mu$ and $D \leftarrow f$
2. **repeat**
3. **while** $D \equiv 0 \pmod{x}$ **do**
4. $D \leftarrow D/x$
5. **if** $U(x) \equiv 0 \pmod{x}$ **then** $U(x) \leftarrow U(x)/x$
6. **else** $U(x) \leftarrow \big(U(x) + \mu(x)\big)/x$
7. **if** $D = 1$ **then break**
8. **if** $\deg D < \deg C$ **then**
9. $t \leftarrow D$, $D \leftarrow C$ and $C \leftarrow t$
10. $t \leftarrow U$, $U \leftarrow V$ and $V \leftarrow t$
11. $D \leftarrow C + D$ and $U \leftarrow U + V$
12. **return** $U$

**Remark.** *It is possible to get directly* $g(x)/f(x) \mod \mu(x)$ *by setting* $U \leftarrow g$ *instead of* $U \leftarrow 1$ *in line 1. of Algorithm 2.*

Before explaining the second method, we need to introduce the concept of *addition chains*. An addition chain computing the integer $n$ is a sequence $b = (b_0, \ldots, b_s)$ such that $b_0 = 1, b_s = n$ and $b_i = b_j + b_k$ for all $1 \leqslant i \leqslant s$ and $0 \leqslant j, k \leqslant i - 1$. Addition chains are used to compute exponentiations. The shorter is the chain the faster is the computation of $x^n$. An addition chain can be easily obtained from the square and multiply algorithm, but more sophisticated methods can give shorter chains [BC 1990, BB$^+$ 1989, BBB 1994]. When several exponentiations to the same exponent $n$ occur it is a good idea to spend some time to search for a short addition chain.
Next algorithm has the same asymptotic complexity to get an inverse than the extended Euclidean algorithm but is reported to be a little faster in certain circumstances [NÖC 1996].
Let us explain the principles of the method. We know from Lagrange's theorem that $|\mathbb{F}_{2^n}^\times| = 2^n - 1$. So $\alpha^{2^n-2} = 1/\alpha$. Now

$$2^n - 2 = 2(2^{n-1} - 1)$$

and one can take advantage of an addition chain to compute $n-1$ and of squarings which are easy to compute.

**Algorithm 3.** Inverse of an element of $\mathbb{F}_{2^n}^\times$ using Lagrange's theorem

INPUT: An element $\alpha \in \mathbb{F}_{2^n}$ and an addition chain $(b_0, b_1, \ldots, b_s)$ computing $n-1$.
OUTPUT: The inverse of $\alpha$ *i.e.* $\alpha^{2^n-2} = 1/\alpha$.

1. $T[0] = \alpha$ and $i \leftarrow 1$
2. **while** $i \leqslant s$ **do**
3. $\quad t \leftarrow T[k]^{2^j}$ where $b_i = b_k + b_j$
4. $\quad T[i] = t \cdot T[j]$ $\quad [T[i] = \alpha^{2^{b_i}-1}$ for all $i]$
5. $\quad i \leftarrow i + 1$
6. **return** $T[s]^2$ $\quad [b_s = n-1]$

**Remarks.**

- *In* **Step 3** *note that exchanging $b_k$ and $b_j$ does not alter the correctness of the algorithm. In fact it is better to force $b_k$ to be bigger than $b_j$ so that the exponentiation $T[k]^{2^{b_j}}$ is simpler.*
- *One can obtain the inverse of $\alpha \in \mathbb{F}_{2^n}$ with $2+s$ multiplications in $\mathbb{F}_{2^n}$ and $(1 + \sum_i b_j)$ squarings where $b_j$ appears in $b_i = b_k + b_j$. This last number is equal to $n-1$ when $(b_0, \ldots, b_s)$ is a* star addition chain i.e. *when $b_i = b_{i-1} + b_j$ at each step.*
- *Itoh and Tsujii's method* [IT 1988] *is a special case of Algorithm 3 when the addition chain $b$ is derived from the square and multiply method.*

## 3. Redundant Trinomials

With Algorithm 1, the product of two elements in $\mathbb{F}_{2^n}$ can be reduced with at most $4(n-1)$ elementary operations using trinomials and at most $8(n-1)$ operations using pentanomials.
For some even extension degrees there is an even better choice, namely *all one polynomials*. They are of the form

$$\mu(x) = x^n + x^{n-1} + \cdots + x + 1.$$

Such a $\mu(x)$ is irreducible if and only if $n+1$ is prime and 2 is a primitive element of $\mathbb{F}_{n+1}$. This occurs for 470 values of $n$ up to $10,000$.
It is clear from the definition of $\mu(x)$ that $\mu(x)(x+1) = x^{n+1}+1$. Thus an element of $\mathbb{F}_{2^n}$ can be represented on the *anomalous basis* $(\alpha, \alpha^2, \ldots, \alpha^n)$ where $\alpha$ is a root of $\mu(x)$. In other words an element of $\mathbb{F}_{2^n}$ is represented by a polynomial of degree at most $n$ with no constant coefficient, the unity element 1 being replaced by $x + x^2 + \cdots + x^n$.
The reduction is made modulo $x^{n+1}+1$ and a squaring is simply a permutation of the coordinates. In one sense computations in $\mathbb{F}_{2^n}$ are performed in the ring $\mathbb{F}_2[x]/(x^{n+1}+1)$. Unfortunately this very particular and favorable choice does not apply very well to odd degrees. When $n$ is odd, one can always embed $\mathbb{F}_{2^n}$ in a

cyclotomic ring $\mathbb{F}_2[x]/(x^m+1)$. But $m \geqslant 2n+1$ so that the benefits obtained from a cheap reduction are partially obliterated by a more expensive multiplication [WH$^+$]. Note that for elliptic and hyperelliptic curve cryptography only prime degree extensions are relevant [Fre 2001, GHS 2002, MQ 2001].

We now adopt this idea and transfer it to the setting of polynomial bases. When there is no irreducible trinomial for some extension degree $n$ one can try to find a trinomial $t(x) = x^m + x^k + 1$ with $m$ slightly bigger than $n$ such that $t(x)$ admits an irreducible factor $\mu(x)$ of degree $n$. Such a trinomial is called a *redundant trinomial*. The idea is then to embed $\mathbb{F}_{2^n} \sim \mathbb{F}_2[x]/\big(\mu(x)\big)$ into $\mathbb{F}_{2^n} \sim \mathbb{F}_2[x]/\big(t(x)\big)$. From a practical point of view an element of $\mathbb{F}_{2^n}$ is represented on the redundant basis $1, \alpha, \ldots, \alpha^{m-1}$ where $\alpha$ is a root of $\mu(x)$ and the computations are reduced modulo $t(x)$. As $\mu(x)$ divides $t(x)$, one can reduce modulo $\mu(x)$ at any time and obtain coherent results. If $m-n$ is sufficiently small then the multiplication of two polynomials of degree less than $m$ has the same cost as the multiplication of two polynomials of degree less than $n$, since multiplications are performed at a word level.

To reduce the results one needs at most 2 iterations using Algorithm 1 since one can always choose $t(x) = x^m + x^k + 1$ such that $k \leqslant \lfloor m/2 \rfloor$. Indeed if $k > \lfloor m/2 \rfloor$ the reciprocal polynomial of $t(x)$ can be considered instead.

However with these settings, the expression of a field element is no longer unique, but the result can of course be reduced modulo $\mu(x)$, when it is required. Note that it is possible to perform a fast reduction modulo $\mu(x)$ knowing only $t(x)$ and $\delta(x) = t(x)/\mu(x)$. The same kind of idea provide a quick way to test if two polynomials represent the same field element. Finally, one examines how inversion algorithms behave with this representation.

These topics are discussed in the next section.

## 4. Efficient Implementation of Redundant Trinomials

To reduce a polynomial $f(x)$ modulo $\mu(x)$ one could perform the Euclidean division of $f(x)$ by $\mu(x)$, but this method has a major drawback. It obliges to determine $\mu(x)$ which is not sparse in general. Writing $f(x) = q(x)\mu(x)+r(x)$ then $f(x)\delta(x) = q(x)t(x) + r(x)\delta(x)$ so that

$$f(x) \bmod \mu(x) = \frac{f(x)\delta(x) \bmod t(x)}{\delta(x)}.$$

The last division is exact and can be obtained by an Algorithm derived from Jebelean's one for integers [Jeb 1993] which operates from the least to the most significant bits of $f$.

**Algorithm 4.** Exact division for polynomials in $\mathbb{F}_2[x]$

Input: The non-nil polynomials $f(x)$ and $g(x)$ such that $g(x) \mid f(x)$.
Output: The quotient $q(x)$ such that $q(x) = f(x)/g(x)$.

1. **while** $g(0) = 0$ **do** $f(x) \leftarrow f(x)/x$ and $g(x) \leftarrow g(x)/x$
2. $n \leftarrow \deg f - \deg g$, $q \leftarrow 0$ and $i \leftarrow 0$
3. **while** $i \leqslant n$ **do**
4. **while** $f(0) = 0$ **do** $f(x) \leftarrow f(x)/x$ and $i \leftarrow i+1$

5. $q(x) \leftarrow q(x) + x^i$
6. $f(x) \leftarrow \big(f(x) + g(x)\big)/x$
7. **return** $q(x)$ [if $f(x) \neq 0$ the division was not exact]

---

Two elements $f_1(x)$ and $f_2(x)$ correspond to the same element in $\mathbb{F}_{2^n}$ if and only if $\mu(x) \mid \big(f_1(x) + f_2(x)\big)$. This implies that $t(x) \mid \delta(x)\big(f_1(x) + f_2(x)\big)$. One could use Algorithm 4 to determine whether the division is exact or not but there is a more efficient way to proceed. First note that if $f_1(x)$ and $f_2(x)$ are both of degree at most $m-1$ then

$$\deg\big(\delta(x)\big(f_1(x) + f_2(x)\big)\big) \leqslant 2m - n - 1.$$

So the quotient $q(x)$ of the division of $\delta(x)\big(f_1(x) + f_2(x)\big)$ by $t(x) = x^m + x^k + 1$ is of degree at most $m - n - 1$. Writing the division explicitly we see that if

$$m - k > m - n - 1$$

then $q(x)$ is equal to the quotient of the division of $\delta(x)\big(f_1(x) + f_2(x)\big)$ by $x^m$. This is just a shift and it is simple matter to determine whether $\delta(x)\big(f_1(x) + f_2(x)\big)$ is equal to $q(x)(x^m + x^k + 1)$ or not.
Now one can check, *cf.* Section 6, that all the redundant trinomials found for $n$ up to $10,000$ satisfy $m - k > m - n - 1$.
Concerning inversion, it is clear that Algorithm 3 works without any problem with redundant polynomials. One must be careful with Algorithm 2. Let $\alpha \in \mathbb{F}_{2^n}$ be represented by $f(x)$. When the algorithm returns $u$ and $v$ such that

$$f(x)u(x) + t(x)v(x) = 1$$

then the inverse of $\alpha$ is given by $u(x)$. But one could have

$$f(x)u(x) + t(x)v(x) = d(x)$$

with $\deg d(x) > 0$. In this case two possibilities arise. If $\mu(x) \mid d(x)$, which can be checked by looking at the degree of $d(x)$, then $\alpha = 0$. Otherwise $d(x) \mid \delta(x)$ and the inverse of $\alpha$ is given by $u(x)e(x)$ where $e(x)$ is the inverse of $d(x)$ modulo $\mu(x)$. Nevertheless there is a more simple technique. Indeed $t(x)$ is squarefree. So the gcd of $f(x)\delta(x)$ and $t(x)$ is equal to $\delta(x)$ and

$$f(x)\delta(x)u_1(x) + t(x)v_1(x) = \delta(x)$$

so that

$$f(x)u_1(x) + \mu(x)v_1(x) = 1$$

and the inverse of $f(x)$ is directly given by $u_1(x)$. The degree of $\delta(x)$ is usually much smaller than the degree of $e(x)$. So the multiplication is faster. No reduction modulo $t(x)$ is required at the end. It is not necessary to compute or precompute anything new. Even when $\gcd\big(f(x), t(x)\big) = 1$ this last techniques works. So one can either compute the extended $\gcd\big(f(x), t(x)\big)$, test its value and compute the extended $\gcd\big(f(x)\delta(x), t(x)\big)$ if necessary, or always perform only this last computation. The tradeoff in time depends on the number of irreducible factors of $\delta$ and the cost of a modular multiplication. Indeed the degree and the number of factors of $\delta(x)$ determine the probability that a random polynomial is prime to $t(x)$. If $\delta(x)$ is irreducible of degree $r$ then this probability is clearly equal to $1 - 1/2^r$. If $\delta(x)$ has two factors of degree $r_1$ and $r_2$, necessarily distinct since $t(x)$ is squarefree,

the probability becomes $1 - 1/2^{r_1} - 1/2^{r_2} + 1/2^{r_1+r_2}$. By induction, if $\delta(x)$ has $\ell$ distinct factors of degree $r_1, r_2, \ldots, r_\ell$ then the probability that $t(x) = x^m + x^k + 1$ is prime to a random polynomial of degree less than $m$ is

$$1 \quad - \sum_{\substack{n=1 \\ 1 \leqslant i_1 < \cdots < i_n \leqslant \ell}}^{\ell} \frac{(-1)^n}{2^{r_{i_1} + \cdots + r_{i_n}}}.$$

Note that $\delta(x)$ is irreducible in about 95% of the cases, *cf.* Section 6.

## 5. Example

Let us consider $\mathbb{F}_{2^8}$. There is no trinomial of degree 8 irreducible over $\mathbb{F}_2$. Instead one usually chooses the irreducible pentanomial $p(x) = x^8 + x^4 + x^3 + x + 1$. Nevertheless it is easily seen that $t(x) = x^{11} + x^5 + 1$ splits as $\mu(x)$ times $\delta(x)$ where $\mu(x) = x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$ and $\delta(x) = x^3 + x + 1$ are both irreducible. The explicit expression of $\mu(x)$ is not important. In fact $t(x)$ and $\delta(x) = x^3 + x + 1$ are enough to compute in $\mathbb{F}_{2^8}$.

Let $f(x)$ and $g(x)$ be two polynomials of degree 7, namely

$$f(x) = x^7 + x^6 + x^2 + x + 1$$

and

$$g(x) = x^7 + x^6 + x^3 + x^2 + x + 1.$$

The product of $f(x)$ and $g(x)$ reduced modulo $t(x)$ is $h(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + x + 1$, whereas it is equal to $x^6 + x^4 + x^2 + 1$ modulo $\mu(x)$. Of course $h(x) \equiv x^6 + x^4 + x^2 + 1 \pmod{\mu(x)}$ but there is no need to reduce $h(x)$ at this stage.

Now let us compute the inverse of $f(x)$ and $g(x)$. Using Algorithm 2, one gets

$$f(x)(x^9 + x^8 + x^7 + x^4 + x^2 + x + 1) + t(x)(x^5 + x^2) = 1$$

and

$$g(x)(x^4 + x^3 + x^2 + x) + t(x) = x^3 + x + 1.$$

We conclude immediately that the inverse of $f(x)$ is

$$f(x)^{-1} \equiv x^9 + x^8 + x^7 + x^4 + x^2 + x + 1 \pmod{t(x)}.$$

For the inverse of $g(x)$ one can first multiply $g(x)$ with $\delta(x)$ and compute an extended Euclidean gcd again. We get

$$g(x)\delta(x)(x^6 + x^5 + x^2 + 1) + t(x)(x^5 + x^2 + x) = x^3 + x + 1$$

so that

$$g(x)^{-1} \equiv x^6 + x^5 + x^2 + 1 \pmod{t(x)}.$$

With Algorithm 3, one gets directly

$$f(x)^{-1} \equiv f(x)^{2^8-2} \equiv x^3 + x^2 + x \pmod{t(x)}$$

and

$$g(x)^{-1} \equiv g(x)^{2^8-2} \equiv x^{10} + x^9 + x^5 \pmod{t(x)}.$$

The results are different representations of the same elements. If one wants to check it out, for example for the inverse of $f(x)$, it is enough to compute

$$(x^3 + x + 1)\big((x^9 + x^8 + x^7 + x^4 + x^2 + x + 1 + x^3 + x^2 + x) + (x^3 + x^2 + x)\big)$$

which is equal to $x^{12}+x^{11}+x^6+x^5+x+1$ and test if this polynomial is a multiple of $t(x)$. If so the quotient must be $x+1$ and indeed

$$(x+1)(x^{11}+x^5+1) = x^{12}+x^{11}+x^6+x^5+x+1$$

so that

$$x^9+x^8+x^7+x^4+x^2+x+1+x^3+x^2+x \equiv x^3+x^2+x \pmod{\mu(x)}.$$

## 6. Results

An exhaustive search of redundant trinomials has been conducted using `NTL` [NTL] for extension degrees $n \leqslant 10,000$ when no irreducible trinomial exist. More precisely, given $n$ we try to find a trinomial $t(x) = x^m + x^k + 1$ such that

- $t(x)$ has an irreducible factor of degree $n$
- $m$ is a small as possible
- $k$ is as small as possible.

It turns out that such a polynomial always exists for the investigated range of degree, *cf.* the next Table. To simplify the search one notes that such a trinomial is necessarily squarefree. Indeed $\gcd(t(x), t'(x))$ is equal to 1 when $m$ or $k$ is odd. Both $m$ and $k$ cannot be even otherwise $x^m + x^k + 1 = (x^{m/2} + x^{k/2} + 1)^2$ and one should have chosen $x^{m/2} + x^{k/2} + 1$ instead.
Then the idea is to test all the trinomials $x^m + x^k + 1$ with $n+1 \leqslant m$ and $1 \leqslant k \leqslant \lfloor m/2 \rfloor$ until a good candidate is found, that is a trinomial with a factor of degree $m-n$.
It is well known that $x^{2^k} + x$ is equal to the product of all irreducible polynomials of degree $d$ such that $d \mid k$. Since $t(x)$ is squarefree it is easy to determine if it has a factor $\delta(x)$ of degree $m-n$, computing $\gcd\big(x^{2^i} + x, x^m + x^k + 1\big)$ for successive $i \leqslant m-n$. Note that such a gcd computation can be very costly when $m-n$ is large. It is much faster to compute $g(x) \equiv x^{2^i} \pmod{t(x)}$ by successive squarings and reductions first and then $\gcd\big(g(x)+x, t(x)\big)$. If $t(x)$ has a factor $\delta(x)$ of degree $m-n$ the irreducibility of $t(x)/\delta(x)$ is finally checked.
For all the extensions up to the degree $10,000$ which do not have an irreducible trinomial and our proposal provides a redundant trinomial. There are 4748 such extensions. Note that when an all one polynomial is available it is given even if an irreducible trinomial exists for that extension degree.
The following Tables contain the redundant trinomials found or all one polynomials when they exist. In total 5218 extensions are given.
The redundant trinomials $x^m+x^k+1$ where $m = n+\deg\delta$ and the all one polynomial $(x^{n+1}+1)/(x+1)$ are respectively represented by $n, \deg\delta, k$ and $n, 1$. The degree of $\delta$ is rather small in general. In about 95% of the cases it is less than or equal to 10. It is maximum for $n = 5373$ and equals 40.

| $\deg\delta$ | 1 | 2 | 3 | 4 | 5 | $\leqslant 10$ | $\leqslant 20$ | $\leqslant 30$ | $\leqslant 40$ |
|---|---|---|---|---|---|---|---|---|---|
| # | 470 | 1278 | 1569 | 130 | 646 | 4969 | 5206 | 5216 | 5218 |

In about 87% of the cases $\delta$ is irreducible. With 32-bit processors, redundant trinomials require the same number of words as an irreducible polynomial of degree $n$ in more than 86% of the cases to represent field elements. Otherwise one more

word is necessary, except for the extension of degree 5373 which needs two more words.
For each degree, the factor $\delta$ is not explicitly given in the Tables, but it is easy to retrieve since

$$\delta(x) = \gcd\left(x^m + x^k + 1, \prod_{i=1}^{m-n}\left(x^{2^i} + x\right)\right).$$

Also $\delta(x)$ can be found by trial divisions when its degree is small.
The complete data, including the expression of $\delta(x)$, are available on the internet [Doche].

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2,1 | 4,1 | 8,3,5 | 10,1 | 12,1 | 13,3,3 | 16,3,4 | 18,1 | 19,3,3 | 24,3,4 |
| 26,3,12 | 27,2,1 | 28,1 | 32,5,16 | 36,1 | 37,6,4 | 38,2,17 | 40,3,3 | 43,10,2 | 45,7,9 |
| 48,3,20 | 50,3,5 | 51,2,4 | 52,1 | 53,8,28 | 56,2,5 | 58,1 | 59,2,26 | 60,1 | 61,5,17 |
| 64,7,12 | 66,1 | 67,9,29 | 69,3,13 | 70,7,11 | 72,3,8 | 75,2,4 | 77,3,9 | 78,2,31 | 80,3,11 |
| 82,1 | 83,2,14 | 85,8,28 | 88,8,19 | 91,8,1 | 96,2,1 | 99,2,13 | 100,1 | 101,2,2 | 104,5,9 |
| 106,1 | 107,2,8 | 109,9,21 | 112,3,22 | 114,3,4 | 115,10,6 | 116,5,17 | 117,6,31 | 120,2,25 | 122,3,9 |
| 125,3,3 | 128,2,17 | 130,1 | 131,7,61 | 133,3,43 | 136,3,30 | 138,1 | 139,3,3 | 141,3,13 | 143,3,53 |
| 144,7,19 | 148,1 | 149,2,2 | 152,2,65 | 157,7,25 | 158,5,19 | 160,3,27 | 162,1 | 163,8,70 | 164,5,59 |
| 165,5,9 | 168,3,1 | 171,2,10 | 172,1 | 173,3,5 | 176,2,53 | 178,1 | 179,2,14 | 180,1 | 181,7,51 |
| 184,3,60 | 187,7,45 | 188,4,61 | 189,3,37 | 190,4,33 | 192,3,53 | 195,2,25 | 196,1 | 197,3,69 | 200,5,42 |
| 203,7,73 | 205,5,29 | 206,2,17 | 208,3,45 | 210,1 | 211,3,103 | 213,3,37 | 216,3,101 | 219,2,1 | 221,15,77 |
| 222,2,37 | 224,3,86 | 226,1 | 227,2,77 | 229,3,61 | 230,2,35 | 232,3,69 | 235,14,7 | 237,3,41 | 240,2,37 |
| 243,2,52 | 245,2,2 | 246,2,109 | 248,2,41 | 251,2,74 | 254,2,71 | 256,16,45 | 259,5,103 | 261,3,109 | 262,4,89 |
| 264,3,68 | 267,2,88 | 268,1 | 269,5,47 | 272,3,87 | 275,3,99 | 277,6,12 | 280,5,103 | 283,3,51 | 285,6,122 |
| 288,2,133 | 290,3,114 | 291,2,31 | 292,1 | 293,2,2 | 296,5,15 | 298,7,91 | 299,2,5 | 301,6,78 | 304,3,46 |
| 306,8,55 | 307,5,119 | 309,7,87 | 311,8,139 | 312,9,143 | 315,2,127 | 316,1 | 317,3,113 | 320,3,26 | 323,2,41 |
| 325,3,151 | 326,2,5 | 328,3,52 | 331,13,69 | 334,5,115 | 335,6,20 | 336,3,1 | 338,3,32 | 339,2,13 | 341,10,124 |
| 344,2,125 | 346,1 | 347,2,173 | 348,1 | 349,6,177 | 352,3,78 | 355,11,173 | 356,15,38 | 357,3,79 | 360,3,53 |
| 361,8,64 | 363,2,169 | 365,3,89 | 368,8,55 | 371,2,56 | 372,1 | 373,3,85 | 374,2,5 | 376,3,159 | 378,1 |
| 379,3,187 | 381,8,99 | 384,3,94 | 387,2,67 | 388,1 | 389,5,193 | 392,3,71 | 395,11,187 | 397,5,13 | 398,9,203 |
| 400,3,159 | 403,5,127 | 405,3,13 | 408,9,90 | 410,4,107 | 411,5,105 | 413,3,9 | 416,6,15 | 418,1 | 419,2,176 |
| 420,1 | 421,8,14 | 424,9,112 | 427,5,5 | 429,3,137 | 430,8,91 | 432,3,38 | 434,3,170 | 435,2,61 | 437,6,12 |
| 440,3,146 | 442,1 | 443,10,68 | 445,5,193 | 448,3,78 | 451,7,139 | 452,7,211 | 453,3,227 | 454,5,10 | 456,2,25 |
| 459,2,202 | 460,1 | 461,3,27 | 464,2,101 | 466,1 | 467,2,29 | 469,8,109 | 472,3,214 | 475,5,133 | 477,3,89 |
| 480,7,224 | 482,3,108 | 483,2,16 | 485,7,181 | 488,3,180 | 490,1 | 491,2,224 | 493,3,37 | 496,3,66 | 499,16,137 |
| 501,10,101 | 502,5,70 | 504,5,167 | 507,2,49 | 508,1 | 509,12,204 | 512,9,252 | 515,2,5 | 517,5,65 | 520,3,18 |
| 522,1 | 523,3,3 | 525,10,89 | 528,3,121 | 530,3,24 | 531,2,226 | 533,3,195 | 535,7,25 | 536,2,113 | 539,2,92 |
| 540,1 | 541,6,37 | 542,2,209 | 544,5,215 | 546,1 | 547,7,131 | 548,2,107 | 549,5,261 | 552,2,133 | 554,3,27 |
| 555,2,58 | 556,1 | 557,8,12 | 560,3,99 | 562,1 | 563,2,86 | 565,3,3 | 568,3,40 | 571,5,187 | 572,5,281 |
| 573,5,249 | 576,2,169 | 578,9,153 | 579,2,148 | 581,11,241 | 584,3,72 | 586,1 | 587,2,104 | 589,3,97 | 591,8,67 |
| 592,7,37 | 595,3,135 | 597,7,257 | 598,5,13 | 600,2,145 | 603,2,4 | 605,3,219 | 608,3,48 | 611,2,11 | 612,1 |
| 613,10,76 | 616,3,64 | 618,1 | 619,5,265 | 621,3,283 | 624,2,193 | 627,5,261 | 629,3,269 | 630,2,37 | 632,2,281 |
| 635,2,290 | 637,3,127 | 638,2,89 | 640,7,23 | 643,5,191 | 644,2,287 | 645,3,103 | 648,5,26 | 652,1 | 653,3,155 |
| 656,2,125 | 658,1 | 659,2,80 | 660,1 | 661,3,81 | 664,3,297 | 666,3,173 | 667,3,211 | 669,5,139 | 672,3,8 |
| 674,3,186 | 675,8,219 | 676,1 | 677,3,59 | 678,2,169 | 680,2,269 | 681,2,193 | 683,2,47 | 685,3,255 | 688,3,204 |
| 691,14,298 | 693,8,258 | 696,3,95 | 699,2,160 | 700,1 | 701,3,167 | 703,3,25 | 704,5,169 | 706,3,34 | 707,2,74 |
| 708,1 | 709,3,123 | 710,2,251 | 712,3,136 | 715,7,165 | 717,6,110 | 720,3,251 | 723,3,295 | 725,8,168 | 728,2,53 |
| 731,2,146 | 733,3,45 | 734,4,329 | 736,3,174 | 739,7,27 | 741,7,83 | 744,2,49 | 747,2,241 | 749,8,205 | 752,2,353 |
| 755,2,98 | 756,1 | 757,3,97 | 760,5,46 | 763,3,247 | 764,4,299 | 765,3,127 | 766,5,130 | 768,3,19 | 770,3,44 |
| 771,2,103 | 772,1 | 773,3,11 | 776,3,132 | 779,2,161 | 781,6,375 | 784,9,86 | 786,1 | 787,3,67 | 788,9,266 |
| 789,10,276 | 790,5,136 | 792,2,325 | 795,2,169 | 796,1 | 797,7,347 | 800,2,77 | 802,7,341 | 803,2,89 | 805,3,219 |
| 808,6,403 | 811,5,161 | 813,3,181 | 816,5,288 | 819,2,313 | 820,1 | 821,6,363 | 824,2,149 | 826,1 | 827,2,68 |
| 828,1 | 829,3,291 | 830,2,323 | 832,3,94 | 835,5,101 | 836,2,275 | 837,5,223 | 840,3,155 | 843,2,187 | 848,2,341 |
| 851,2,119 | 852,1 | 853,3,307 | 854,2,161 | 856,3,235 | 858,1 | 859,9,197 | 863,6,300 | 864,5,144 | 867,2,25 |
| 869,3,75 | 872,9,27 | 874,6,111 | 875,2,392 | 876,1 | 877,10,69 | 878,7,341 | 880,3,61 | 882,1 | 883,5,395 |
| 885,3,137 | 886,9,314 | 888,3,241 | 891,2,442 | 893,5,59 | 896,3,65 | 899,2,329 | 901,6,1 | 904,3,6 | 906,1 |
| 907,7,105 | 909,3,55 | 910,7,131 | 912,2,337 | 914,9,369 | 915,2,349 | 917,3,9 | 920,3,375 | 922,3,229 | 923,2,389 |
| 925,12,18 | 928,7,64 | 929,2,302 | 931,10,415 | 933,3,1 | 934,5,428 | 936,2,25 | 939,2,67 | 940,1 | 941,3,317 |
| 944,2,125 | 946,1 | 947,2,50 | 949,8,38 | 950,2,383 | 952,3,324 | 955,7,321 | 957,3,367 | 958,7,174 | 960,2,241 |
| 962,3,464 | 963,2,7 | 965,3,293 | 968,2,29 | 970,7,226 | 971,2,179 | 973,12,233 | 974,7,65 | 976,3,394 | 978,3,425 |
| 980,5,11 | 981,5,235 | 984,2,313 | 987,2,28 | 989,3,11 | 992,5,472 | 995,2,89 | 997,3,319 | 1000,9,140 | 1002,3,41 |
| 1003,8,362 | 1004,5,68 | 1005,6,74 | 1006,5,206 | 1008,7,59 | 1011,2,163 | 1013,3,101 | 1016,3,209 | 1017,2,505 | 1018,1 |
| 1019,2,290 | 1021,3,69 | 1024,3,22 | 1027,9,477 | 1032,5,252 | 1035,2,181 | 1037,3,201 | 1038,2,73 | 1040,2,353 | 1043,2,218 |
| 1045,6,37 | 1046,5,333 | 1048,8,337 | 1051,7,475 | 1053,3,247 | 1056,3,335 | 1059,2,268 | 1060,1 | 1061,5,261 | 1064,2,89 |
| 1066,11,187 | 1067,2,101 | 1068,4,223 | 1069,9,355 | 1070,2,455 | 1072,3,13 | 1073,2,29 | 1074,3,32 | 1075,9,119 | 1076,5,8 |
| 1077,3,391 | 1080,3,358 | 1083,2,1 | 1088,2,329 | 1090,1 | 1091,2,134 | 1093,3,75 | 1096,7,167 | 1099,5,259 | 1101,7,157 |
| 1104,3,530 | 1107,2,76 | 1108,1 | 1109,6,281 | 1112,3,6 | 1114,3,244 | 1115,2,407 | 1116,1 | 1117,7,499 | 1118,2,377 |
| 1120,5,149 | 1122,1 | 1123,3,291 | 1124,2,71 | 1125,6,10 | 1128,2,61 | 1131,2,250 | 1132,4,449 | 1133,3,461 | 1136,6,275 |
| 1139,2,155 | 1141,5,329 | 1143,3,505 | 1144,3,198 | 1147,5,287 | 1149,5,499 | 1150,5,344 | 1152,9,282 | 1155,3,527 | 1157,3,431 |
| 1160,3,159 | 1162,12,309 | 1163,2,131 | 1165,6,411 | 1168,3,90 | 1170,1 | 1171,7,5 | 1172,2,191 | 1173,7,191 | 1176,2,205 |
| 1179,2,118 | 1181,6,491 | 1184,5,19 | 1186,1 | 1187,5,345 | 1189,8,575 | 1192,3,144 | 1194,4,427 | 1195,5,241 | 1197,5,33 |
| 1200,3,11 | 1203,2,148 | 1205,12,527 | 1208,5,25 | 1211,2,197 | 1212,1 | 1213,3,309 | 1216,3,117 | 1219,4,2 | 1221,7,351 |
| 1222,5,107 | 1224,2,289 | 1227,2,133 | 1228,1 | 1229,5,143 | 1232,2,581 | 1235,2,338 | 1236,1 | 1237,3,619 | 1240,3,369 |
| 1243,8,296 | 1244,2,311 | 1245,10,69 | 1248,3,239 | 1250,5,584 | 1251,2,34 | 1253,3,15 | 1254,2,67 | 1256,2,545 | 1258,1 |
| 1259,2,20 | 1261,3,349 | 1262,2,245 | 1264,6,187 | 1267,7,437 | 1269,5,597 | 1272,3,248 | 1274,5,407 | 1275,2,433 | 1276,1 |
| 1277,7,127 | 1280,2,233 | 1282,1 | 1283,3,323 | 1285,5,49 | 1288,5,565 | 1290,1 | 1291,8,44 | 1292,5,80 | 1293,3,607 |
| 1296,3,475 | 1299,2,148 | 1300,1 | 1301,5,273 | 1303,4,248 | 1304,2,605 | 1306,1 | 1307,2,62 | 1309,5,209 | 1312,3,163 |
| 1315,5,479 | 1316,5,386 | 1317,3,47 | 1318,5,68 | 1320,9,438 | 1322,5,398 | 1323,2,208 | 1325,5,33 | 1328,3,171 | 1330,3,169 |
| 1331,2,101 | 1333,11,79 | 1336,3,90 | 1339,12,541 | 1341,9,227 | 1342,5,199 | 1344,2,457 | 1346,3,81 | 1347,3,79 | 1349,5,585 |
| 1352,3,12 | 1355,2,260 | 1357,3,129 | 1360,3,253 | 1363,9,149 | 1365,12,599 | 1368,3,86 | 1370,3,600 | 1371,2,364 | 1372,1 |
| 1373,3,257 | 1376,11,501 | 1378,3,570 | 1379,2,236 | 1380,1 | 1381,6,562 | 1382,2,5 | 1384,3,45 | 1387,11,401 | 1389,3,193 |
| 1392,2,625 | 1394,3,194 | 1395,2,304 | 1397,5,501 | 1400,2,89 | 1403,5,151 | 1405,8,260 | 1406,7,281 | 1408,5,203 | 1411,10,6 |
| 1413,10,115 | 1416,5,468 | 1418,4,491 | 1419,2,205 | 1421,3,141 | 1424,2,65 | 1426,1 | 1427,2,113 | 1429,8,715 | 1432,5,499 |
| 1435,14,671 | 1437,7,31 | 1439,4,179 | 1440,3,257 | 1443,2,241 | 1445,3,191 | 1448,3,62 | 1450,1 | 1451,2,686 | 1452,1 |
| 1453,7,91 | 1456,3,610 | 1459,12,423 | 1461,3,101 | 1462,5,554 | 1464,2,721 | 1467,2,181 | 1469,8,363 | 1472,2,725 | 1474,7,232 |
| 1475,2,272 | 1477,12,589 | 1480,3,492 | 1482,1 | 1483,9,725 | 1484,2,407 | 1485,5,381 | 1488,9,198 | 1491,2,145 | 1492,1 |
| 1493,3,333 | 1494,8,387 | 1496,2,41 | 1498,1 | 1499,3,663 | 1501,3,207 | 1502,2,83 | 1504,5,58 | 1506,3,55 | 1507,3,739 |
| 1509,7,395 | 1512,3,211 | 1515,2,142 | 1517,3,101 | 1520,7,241 | 1522,1 | 1523,2,206 | 1525,6,300 | 1528,3,88 | 1530,1 |
| 1531,5,199 | 1532,5,215 | 1533,3,485 | 1536,2,409 | 1538,3,227 | 1539,3,479 | 1541,7,299 | 1544,2,605 | 1546,3,115 | 1547,2,380 |
| 1548,1 | 1549,3,529 | 1552,3,171 | 1555,12,606 | 1557,7,513 | 1560,3,220 | 1563,2,364 | 1565,8,348 | 1568,3,443 | 1570,1 |
| 1571,2,101 | 1573,3,663 | 1574,5,57 | 1576,7,532 | 1579,5,191 | 1581,3,503 | 1584,2,37 | 1587,2,370 | 1589,9,599 | 1592,5,781 |
| 1594,3,33 | 1595,2,548 | 1597,3,181 | 1598,7,452 | 1600,5,646 | 1603,5,703 | 1605,3,155 | 1608,2,1 | 1610,17,731 | 1611,2,94 |
| 1613,3,275 | 1614,4,261 | 1616,2,197 | 1618,1 | 1619,3,155 | 1620,1 | 1621,5,49 | 1622,2,473 | 1624,3,289 | 1626,3,274 |
| 1627,3,723 | 1629,7,109 | 1632,2,745 | 1635,2,733 | 1636,1 | 1637,3,689 | 1640,2,317 | 1643,2,632 | 1644,2,43 | 1645,6,61 |
| 1646,2,461 | 1648,3,123 | 1651,3,111 | 1653,3,691 | 1654,5,568 | 1656,2,757 | 1658,3,3 | 1659,2,442 | 1661,6,359 | 1662,5,573 |
| 1664,13,448 | 1666,1 | 1667,2,698 | 1668,1 | 1669,9,21 | 1670,2,629 | 1672,3,468 | 1675,5,47 | 1677,5,569 | 1680,3,190 |
| 1682,3,221 | 1683,8,32 | 1684,4,321 | 1685,3,299 | 1686,2,625 | 1688,3,251 | 1690,3,214 | 1691,2,335 | 1692,1 | 1693,6,555 |
| 1696,3,375 | 1699,7,179 | 1701,8,294 | 1702,4,749 | 1704,3,394 | 1706,3,66 | 1707,2,109 | 1709,5,69 | 1712,5,228 | 1714,3,76 |
| 1715,2,5 | 1717,3,379 | 1718,5,805 | 1720,3,192 | 1723,7,417 | 1725,3,67 | 1727,3,129 | 1728,2,709 | 1730,5,694 | 1731,2,505 |
| 1732,1 | 1733,6,818 | 1736,3,855 | 1739,2,329 | 1740,1 | 1741,6,87 | 1744,3,622 | 1746,1 | 1747,5,785 | 1749,3,713 |
| 1752,3,568 | 1754,5,314 | 1755,2,466 | 1757,2,2 | 1758,2,481 | 1760,3,494 | 1761,2,28 | 1762,3,339 | 1763,2,599 | 1765,3,243 |
| 1766,2,863 | 1768,9,624 | 1771,10,757 | 1773,3,389 | 1776,5,80 | 1779,2,172 | 1781,5,1 | 1784,7,548 | 1786,1 | 1787,2,371 |
| 1789,7,625 | 1792,3,156 | 1794,7,244 | 1795,7,857 | 1796,5,293 | 1797,3,341 | 1800,2,613 | 1803,2,241 | 1805,3,783 | 1808,5,645 |
| 1811,2,746 | 1812,2,679 | 1813,8,211 | 1816,3,354 | 1819,8,190 | 1821,12,718 | 1822,5,799 | 1824,7,642 | 1826,3,143 | 1827,8,807 |
| 1829,3,431 | 1832,2,605 | 1834,6,381 | 1835,10,619 | 1837,5,557 | 1840,3,241 | 1842,6,177 | 1843,3,459 | 1845,6,755 | 1848,3,155 |
| 1850,3,333 | 1851,2,124 | 1852,4,807 | 1853,10,871 | 1856,3,279 | 1858,3,88 | 1859,2,71 | 1860,1 | 1861,6,741 | 1864,3,214 |
| 1866,1 | 1867,3,271 | 1868,4,811 | 1869,6,187 | 1872,7,436 | 1874,6,113 | 1875,2,412 | 1876,1 | 1877,3,747 | 1880,2,209 |
| 1882,7,799 | 1883,2,701 | 1885,3,435 | 1888,3,481 | 1891,3,307 | 1892,2,179 | 1893,3,569 | 1894,5,949 | 1896,3,269 | 1897,7,263 |
| 1898,3,20 | 1899,7,927 | 1900,1 | 1901,12,945 | 1904,2,173 | 1906,1 | 1907,2,455 | 1909,3,423 | 1910,2,137 | 1912,3,957 |
| 1914,3,79 | 1915,11,653 | 1916,2,443 | 1917,3,41 | 1920,3,491 | 1922,9,581 | 1923,2,892 | 1925,6,276 | 1928,5,867 | 1930,1 |
| 1931,2,275 | 1933,9,451 | 1936,9,512 | 1939,7,93 | 1941,3,389 | 1942,5,475 | 1944,2,781 | 1947,2,364 | 1948,1 | 1949,3,611 |
| 1952,2,233 | 1954,7,67 | 1955,2,143 | 1957,6,139 | 1960,3,121 | 1963,9,257 | 1965,3,325 | 1968,3,496 | 1970,3,170 | 1971,2,292 |
| 1972,1 | 1973,6,500 | 1976,3,876 | 1978,1 | 1979,2,359 | 1981,5,629 | 1982,5,181 | 1984,15,632 | 1986,1 | 1987,9,641 |
| 1989,3,349 | 1992,2,985 | 1995,2,250 | 1996,1 | 1997,6,53 | 1998,2,793 | 2000,3,341 | 2002,3,918 | 2003,2,284 | 2005,14,967 |
| 2008,3,969 | 2011,5,911 | 2012,2,227 | 2013,6,1000 | 2014,4,737 | 2016,3,464 | 2018,9,884 | 2019,2,1003 | 2021,3,369 | 2024,2,893 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2026,1 | 2027,2,491 | 2028,1 | 2029,3,307 | 2030,2,911 | 2032,3,186 | 2035,5,263 | 2037,3,631 | 2038,12,163 | 2040,2,469 |
| 2042,4,683 | 2043,13,315 | 2045,3,293 | 2046,5,468 | 2048,5,64 | 2050,3,444 | 2051,2,149 | 2052,1 | 2053,6,982 | 2056,5,734 |
| 2059,3,187 | 2061,3,583 | 2062,5,802 | 2064,2,637 | 2067,2,256 | 2068,1 | 2069,8,940 | 2071,3,409 | 2072,2,233 | 2075,2,290 |
| 2077,3,187 | 2078,2,179 | 2080,3,657 | 2082,1 | 2083,5,61 | 2084,5,239 | 2085,3,73 | 2088,3,211 | 2090,5,838 | 2091,2,526 |
| 2092,10,397 | 2093,3,491 | 2096,3,389 | 2098,1 | 2099,2,245 | 2101,3,489 | 2104,13,168 | 2107,3,1023 | 2108,4,251 | 2109,3,127 |
| 2110,4,281 | 2112,2,601 | 2115,2,34 | 2117,11,631 | 2120,2,113 | 2123,2,707 | 2125,8,1000 | 2128,5,920 | 2130,1 | 2131,8,49 |
| 2133,14,1042 | 2134,7,638 | 2136,3,544 | 2138,3,51 | 2139,2,112 | 2140,1 | 2141,6,920 | 2144,3,606 | 2147,2,608 | 2149,3,1051 |
| 2152,3,312 | 2154,3,194 | 2155,8,1048 | 2157,3,251 | 2160,6,755 | 2163,2,574 | 2165,6,296 | 2168,2,521 | 2171,2,68 | 2172,4,829 |
| 2173,3,501 | 2176,3,703 | 2179,3,375 | 2181,5,391 | 2184,3,890 | 2187,2,541 | 2189,6,1059 | 2192,5,106 | 2194,3,1038 | 2195,2,419 |
| 2197,5,917 | 2200,3,39 | 2202,4,559 | 2203,3,355 | 2204,8,575 | 2205,6,26 | 2208,3,697 | 2211,2,490 | 2212,1 | 2213,3,201 |
| 2216,2,113 | 2219,2,149 | 2220,1 | 2221,3,855 | 2223,5,577 | 2224,7,538 | 2226,3,29 | 2227,3,447 | 2229,3,37 | 2232,2,37 |
| 2234,3,482 | 2235,2,88 | 2236,1 | 2237,12,1013 | 2240,9,646 | 2242,1 | 2243,2,308 | 2245,3,45 | 2246,5,256 | 2248,3,174 |
| 2251,7,357 | 2253,5,1027 | 2254,5,13 | 2256,3,508 | 2259,2,484 | 2260,7,491 | 2261,3,1107 | 2264,2,1097 | 2266,1 | 2267,2,32 |
| 2268,1 | 2269,10,488 | 2272,5,173 | 2275,5,517 | 2277,6,727 | 2278,4,789 | 2280,3,31 | 2283,2,958 | 2285,5,637 | 2288,2,449 |
| 2290,11,934 | 2291,2,686 | 2292,1 | 2293,6,775 | 2294,2,515 | 2296,3,604 | 2298,3,526 | 2299,3,975 | 2301,5,857 | 2302,7,917 |
| 2304,2,985 | 2307,2,220 | 2308,1 | 2309,6,849 | 2312,2,1109 | 2315,2,50 | 2317,6,493 | 2320,7,324 | 2323,11,953 | 2325,5,29 |
| 2326,12,85 | 2328,2,253 | 2330,3,521 | 2332,1 | 2333,3,617 | 2336,2,533 | 2338,1 | 2339,2,194 | 2341,3,1047 | 2344,3,87 |
| 2347,5,1075 | 2349,7,657 | 2350,5,266 | 2352,2,109 | 2354,3,375 | 2355,2,34 | 2356,1 | 2357,6,507 | 2360,3,713 | 2362,3,513 |
| 2363,2,944 | 2365,3,871 | 2366,5,766 | 2368,3,291 | 2370,1 | 2371,5,125 | 2373,3,169 | 2374,9,977 | 2376,5,686 | 2379,2,181 |
| 2381,3,173 | 2384,2,1085 | 2386,3,447 | 2387,2,173 | 2388,1 | 2389,9,15 | 2392,3,12 | 2395,3,943 | 2397,10,341 | 2398,7,561 |
| 2400,5,311 | 2403,2,604 | 2405,5,121 | 2406,2,229 | 2408,2,497 | 2411,3,795 | 2413,3,381 | 2416,3,537 | 2419,7,127 | 2421,6,353 |
| 2424,2,109 | 2426,8,459 | 2427,2,547 | 2429,8,874 | 2432,3,417 | 2435,2,410 | 2436,1 | 2437,3,957 | 2440,7,532 | 2443,3,667 |
| 2445,3,1145 | 2446,10,833 | 2448,2,493 | 2451,2,241 | 2453,3,641 | 2456,2,209 | 2458,1 | 2459,2,275 | 2461,8,146 | 2462,2,47 |
| 2464,3,15 | 2466,1 | 2467,9,551 | 2469,5,379 | 2471,5,239 | 2472,3,881 | 2475,2,55 | 2476,1 | 2477,3,857 | 2480,6,347 |
| 2482,13,829 | 2483,2,134 | 2486,2,1007 | 2488,5,776 | 2490,3,416 | 2491,3,223 | 2493,3,677 | 2494,5,545 | 2496,2,73 | 2498,3,1074 |
| 2499,2,964 | 2501,7,769 | 2504,2,449 | 2506,3,58 | 2507,2,629 | 2509,3,177 | 2512,3,339 | 2515,3,1159 | 2517,8,458 | 2518,13,182 |
| 2520,2,985 | 2522,3,284 | 2523,2,34 | 2524,4,347 | 2525,3,285 | 2528,3,41 | 2530,1 | 2531,2,281 | 2532,5,163 | 2533,8,479 |
| 2535,3,433 | 2536,3,862 | 2538,1 | 2539,7,581 | 2541,3,1163 | 2544,3,977 | 2547,2,34 | 2548,1 | 2549,13,415 | 2552,15,549 |
| 2555,2,638 | 2556,1 | 2557,9,529 | 2558,2,551 | 2560,3,1137 | 2563,13,163 | 2565,5,581 | 2568,3,97 | 2570,3,174 | 2571,5,5 |
| 2573,8,903 | 2576,3,197 | 2578,1 | 2579,2,23 | 2581,3,885 | 2582,2,377 | 2584,3,96 | 2587,10,48 | 2588,8,797 | 2589,3,265 |
| 2592,2,877 | 2595,2,472 | 2597,9,589 | 2600,3,828 | 2602,3,129 | 2603,2,41 | 2605,3,999 | 2608,5,242 | 2611,11,1243 | 2612,5,548 |
| 2613,7,257 | 2616,2,997 | 2619,2,7 | 2620,1 | 2621,3,375 | 2622,5,1260 | 2624,3,678 | 2627,2,707 | 2629,5,1129 | 2632,3,156 |
| 2634,3,883 | 2635,10,384 | 2636,5,650 | 2637,3,1139 | 2638,5,1276 | 2640,9,647 | 2643,2,13 | 2645,3,941 | 2648,3,281 | 2650,6,75 |
| 2651,2,59 | 2653,3,247 | 2654,4,1129 | 2656,3,592 | 2658,1 | 2659,5,119 | 2661,3,1279 | 2662,15,794 | 2664,6,991 | 2669,7,493 |
| 2672,2,89 | 2675,2,797 | 2676,1 | 2677,3,361 | 2678,2,1001 | 2680,3,969 | 2682,1 | 2683,3,403 | 2684,2,1007 | 2685,8,273 |
| 2688,3,1052 | 2690,7,1126 | 2691,3,1243 | 2692,1 | 2693,9,773 | 2696,2,185 | 2698,1 | 2699,2,656 | 2701,3,69 | 2704,3,85 |
| 2705,4,587 | 2706,1 | 2707,5,455 | 2709,6,148 | 2710,5,763 | 2712,3,772 | 2714,3,381 | 2715,2,709 | 2717,3,503 | 2720,2,869 |
| 2723,2,911 | 2725,8,703 | 2726,2,1115 | 2728,3,3 | 2731,5,245 | 2733,6,445 | 2734,4,557 | 2736,2,1273 | 2739,2,724 | 2740,1 |
| 2741,5,899 | 2744,2,317 | 2746,3,463 | 2747,2,1088 | 2749,5,1025 | 2752,3,237 | 2755,5,1253 | 2757,3,311 | 2758,9,359 | 2760,2,373 |
| 2763,5,551 | 2765,6,761 | 2768,3,975 | 2771,2,281 | 2773,3,909 | 2774,2,689 | 2776,5,379 | 2777,2,275 | 2779,7,453 | 2781,10,194 |
| 2782,9,131 | 2784,2,397 | 2787,2,529 | 2788,1 | 2789,3,821 | 2792,2,749 | 2794,3,754 | 2795,2,161 | 2796,1 | 2797,6,564 |
| 2798,5,355 | 2800,3,610 | 2802,1 | 2803,7,717 | 2805,5,967 | 2808,3,1385 | 2810,3,401 | 2811,2,376 | 2813,8,1146 | 2816,2,389 |
| 2818,1 | 2819,2,269 | 2821,3,1017 | 2822,2,17 | 2824,3,1054 | 2827,17,419 | 2829,3,467 | 2830,5,1129 | 2832,6,411 | 2834,4,1159 |
| 2835,2,106 | 2836,1 | 2837,3,53 | 2838,2,1231 | 2840,3,899 | 2842,1 | 2843,2,752 | 2845,8,863 | 2846,9,1363 | 2848,3,300 |
| 2850,1 | 2851,8,1376 | 2853,5,1063 | 2856,11,228 | 2858,3,785 | 2859,2,748 | 2860,1 | 2861,9,251 | 2864,2,929 | 2866,10,269 |
| 2867,2,56 | 2869,6,241 | 2870,2,149 | 2872,5,1318 | 2874,5,1042 | 2875,3,19 | 2877,3,1 | 2880,3,625 | 2883,2,169 | 2885,3,1223 |
| 2886,9,1392 | 2888,5,1225 | 2891,2,329 | 2893,8,502 | 2894,2,359 | 2896,3,222 | 2899,7,1243 | 2901,3,431 | 2902,4,1077 | 2904,2,949 |
| 2907,2,511 | 2908,1 | 2909,8,1143 | 2912,3,372 | 2915,2,125 | 2917,3,159 | 2920,3,349 | 2923,5,1337 | 2924,9,53 | 2925,6,815 |
| 2926,5,154 | 2928,2,1429 | 2930,4,727 | 2931,2,109 | 2932,9,562 | 2933,5,1393 | 2935,4,941 | 2936,10,739 | 2938,1 | 2939,2,23 |
| 2941,7,647 | 2944,6,559 | 2947,3,519 | 2948,7,968 | 2949,5,645 | 2952,6,939 | 2954,3,281 | 2955,2,601 | 2956,1 | 2957,8,394 |
| 2958,2,577 | 2960,2,1121 | 2962,1 | 2963,2,86 | 2965,6,13 | 2968,3,51 | 2971,10,755 | 2973,3,59 | 2974,10,737 | 2976,2,1189 |
| 2979,2,568 | 2981,5,251 | 2984,3,1121 | 2987,2,170 | 2989,3,897 | 2990,2,353 | 2992,5,533 | 2995,7,701 | 2997,3,271 | 3000,2,889 |
| 3002,3,213 | 3003,2,316 | 3005,3,473 | 3006,2,709 | 3008,3,558 | 3010,1 | 3011,2,143 | 3013,6,127 | 3014,2,173 | 3016,3,685 |
| 3018,1 | 3019,3,123 | 3021,6,202 | 3022,7,860 | 3024,5,308 | 3026,3,95 | 3027,2,1210 | 3029,3,101 | 3030,2,1303 | 3032,3,363 |
| 3035,2,521 | 3036,1 | 3037,10,519 | 3040,5,277 | 3043,8,1070 | 3045,5,1377 | 3047,4,253 | 3048,9,566 | 3051,2,541 | 3053,3,1343 |
| 3054,3,1019 | 3055,3,793 | 3056,2,113 | 3059,3,527 | 3061,3,291 | 3064,3,957 | 3066,1 | 3067,13,221 | 3069,6,683 | 3070,4,693 |
| 3072,3,374 | 3074,3,167 | 3075,2,193 | 3077,5,83 | 3080,3,387 | 3082,1 | 3083,2,167 | 3085,3,913 | 3088,3,1020 | 3091,10,68 |
| 3093,6,1409 | 3096,5,173 | 3098,11,1288 | 3099,2,100 | 3101,15,1055 | 3104,3,599 | 3106,18,137 | 3107,2,221 | 3109,3,307 | 3112,5,700 |
| 3114,3,419 | 3115,3,555 | 3117,3,1541 | 3120,2,757 | 3122,3,303 | 3123,2,124 | 3125,5,1559 | 3128,2,1301 | 3131,2,1487 | 3133,6,564 |
| 3136,3,799 | 3138,3,694 | 3139,3,1495 | 3141,10,587 | 3144,3,13 | 3146,3,1082 | 3147,2,715 | 3149,3,839 | 3152,2,329 | 3154,7,421 |
| 3155,2,1037 | 3157,10,608 | 3158,2,263 | 3160,3,1276 | 3163,8,841 | 3165,3,1105 | 3166,15,212 | 3168,9,1005 | 3171,2,427 | 3173,3,1173 |
| 3176,2,965 | 3179,2,902 | 3181,3,163 | 3184,3,993 | 3186,1 | 3187,5,1129 | 3189,13,647 | 3190,5,689 | 3192,2,1117 | 3195,2,658 |
| 3197,19,889 | 3200,2,1469 | 3202,1 | 3203,2,59 | 3205,3,1333 | 3206,5,1536 | 3208,3,547 | 3211,3,943 | 3213,14,1414 | 3216,5,671 |
| 3218,3,831 | 3219,2,610 | 3221,3,509 | 3224,2,29 | 3226,6,727 | 3227,2,533 | 3229,3,771 | 3231,6,440 | 3232,7,427 | 3235,7,79 |
| 3237,3,23 | 3240,3,1606 | 3242,3,993 | 3243,8,185 | 3245,5,457 | 3248,3,275 | 3250,3,603 | 3251,2,818 | 3252,1 | 3253,3,103 |
| 3256,3,1069 | 3259,11,877 | 3261,10,64 | 3262,5,755 | 3264,3,1037 | 3265,13,125 | 3266,6,537 | 3267,7,571 | 3269,10,977 | 3272,2,989 |
| 3275,2,221 | 3277,3,649 | 3278,4,61 | 3280,6,831 | 3283,12,1052 | 3284,2,551 | 3285,3,1313 | 3288,3,430 | 3290,5,1318 | 3291,8,875 |
| 3293,5,1307 | 3296,5,1075 | 3298,1 | 3299,2,29 | 3301,6,186 | 3304,6,267 | 3306,1 | 3307,7,1563 | 3309,3,353 | 3312,3,719 |
| 3315,2,169 | 3317,6,447 | 3320,3,834 | 3322,1 | 3323,2,1097 | 3325,5,761 | 3328,3,450 | 3331,3,307 | 3333,3,1315 | 3334,5,179 |
| 3336,5,288 | 3339,2,700 | 3340,10,415 | 3341,7,1459 | 3342,2,901 | 3344,2,1073 | 3346,1 | 3347,2,704 | 3349,3,261 | 3352,5,1309 |
| 3354,3,538 | 3355,3,739 | 3357,5,1483 | 3358,7,1407 | 3360,3,1415 | 3361,10,307 | 3362,3,1002 | 3363,2,184 | 3365,6,1226 | 3368,11,1344 |
| 3370,1 | 3371,2,125 | 3373,5,1381 | 3376,3,1009 | 3379,3,1095 | 3381,12,326 | 3384,2,469 | 3386,5,212 | 3387,2,805 | 3389,8,462 |
| 3392,2,197 | 3394,3,363 | 3395,2,29 | 3396,8,1561 | 3397,9,1325 | 3400,3,570 | 3403,10,248 | 3405,9,775 | 3406,5,1624 | 3408,2,673 |
| 3411,2,280 | 3412,1 | 3413,6,1559 | 3416,5,70 | 3419,2,1007 | 3421,6,1095 | 3424,3,124 | 3427,5,985 | 3428,2,1583 | 3429,8,380 |
| 3432,3,172 | 3433,4,804 | 3434,5,143 | 3435,2,421 | 3437,3,407 | 3440,5,76 | 3442,3,712 | 3443,3,1683 | 3445,3,1609 | 3446,5,655 |
| 3448,5,1003 | 3450,5,502 | 3451,5,1711 | 3453,3,589 | 3454,4,197 | 3456,2,1285 | 3459,2,139 | 3460,1 | 3461,3,389 | 3464,3,570 |
| 3466,1 | 3467,2,1100 | 3468,1 | 3469,7,1723 | 3472,7,253 | 3475,3,415 | 3477,12,1664 | 3480,2,445 | 3482,3,228 | 3483,2,1627 |
| 3485,3,143 | 3488,2,161 | 3490,1 | 3491,2,1613 | 3493,8,440 | 3494,5,1099 | 3496,3,163 | 3498,1 | 3499,8,1625 | 3501,10,894 |
| 3502,11,407 | 3504,2,733 | 3506,3,395 | 3507,5,467 | 3508,4,713 | 3509,3,515 | 3512,2,449 | 3514,3,645 | 3515,2,755 | 3516,1 |
| 3517,3,93 | 3518,2,1307 | 3520,3,370 | 3523,5,1157 | 3525,6,34 | 3526,9,194 | 3528,3,617 | 3530,3,582 | 3531,2,769 | 3532,1 |
| 3533,3,227 | 3536,5,202 | 3538,1 | 3539,2,269 | 3541,5,1561 | 3544,3,732 | 3546,1 | 3547,7,1169 | 3549,14,343 | 3552,2,733 |
| 3553,4,279 | 3554,3,738 | 3555,2,1399 | 3556,1 | 3557,3,867 | 3560,7,671 | 3563,2,179 | 3565,3,1047 | 3566,2,233 | 3567,4,454 |
| 3568,3,892 | 3570,1 | 3571,3,279 | 3573,5,199 | 3576,7,500 | 3578,3,489 | 3579,2,988 | 3580,1 | 3581,6,417 | 3584,3,120 |
| 3586,3,1429 | 3587,2,434 | 3589,9,1503 | 3592,3,622 | 3595,5,1099 | 3597,3,1007 | 3598,4,1089 | 3600,2,1381 | 3602,5,38 | 3603,3,635 |
| 3605,12,816 | 3608,3,1136 | 3610,3,474 | 3611,2,317 | 3612,1 | 3613,3,285 | 3616,5,667 | 3619,3,1639 | 3621,7,1601 | 3623,5,1487 |
| 3624,2,1441 | 3626,8,1431 | 3627,2,1084 | 3629,6,1272 | 3632,2,389 | 3635,2,653 | 3636,1 | 3637,6,1194 | 3638,5,286 | 3640,9,378 |
| 3642,1 | 3643,5,221 | 3645,3,1067 | 3646,7,350 | 3648,2,1501 | 3651,2,1762 | 3653,3,1389 | 3656,2,401 | 3658,1 | 3659,2,110 |
| 3661,6,124 | 3664,3,1542 | 3666,11,546 | 3667,7,115 | 3669,3,853 | 3670,5,1478 | 3672,6,867 | 3674,3,1242 | 3675,2,229 | 3676,1 |
| 3677,21,579 | 3680,11,187 | 3683,2,467 | 3685,5,1817 | 3688,3,111 | 3690,1 | 3691,3,1695 | 3692,4,1633 | 3693,5,787 | 3696,2,1 |
| 3699,2,367 | 3700,1 | 3701,6,1010 | 3704,2,1349 | 3707,5,1429 | 3708,1 | 3709,3,349 | 3712,5,367 | 3715,10,903 | 3716,2,263 |
| 3717,10,261 | 3718,4,413 | 3720,2,889 | 3722,3,509 | 3723,2,1036 | 3724,7,1098 | 3725,9,733 | 3728,10,1417 | 3731,10,137 | 3732,1 |
| 3733,6,835 | 3736,3,325 | 3739,15,527 | 3741,3,331 | 3742,5,1843 | 3744,2,253 | 3746,3,635 | 3747,2,988 | 3748,9,1266 | 3749,6,1236 |
| 3752,9,1009 | 3755,5,1141 | 3757,3,1671 | 3758,13,1109 | 3760,3,1006 | 3763,13,1265 | 3765,10,34 | 3766,5,1279 | 3768,5,1455 | 3771,2,382 |
| 3773,3,555 | 3774,2,493 | 3776,3,1250 | 3778,1 | 3779,2,1115 | 3781,3,285 | 3784,5,215 | 3787,3,1311 | 3789,10,291 | 3790,8,1267 |
| 3792,2,1525 | 3794,3,450 | 3795,2,754 | 3796,1 | 3797,6,1145 | 3800,3,38 | 3802,1 | 3803,2,1289 | 3805,6,727 | 3806,2,485 |
| 3808,8,791 | 3811,8,553 | 3813,3,929 | 3814,7,231 | 3816,2,1573 | 3818,3,170 | 3819,2,922 | 3820,7,527 | 3821,5,551 | 3824,7,563 |
| 3826,7,508 | 3827,2,338 | 3829,5,1265 | 3832,3,261 | 3835,10,913 | 3837,3,1307 | 3840,6,699 | 3843,2,901 | 3845,3,477 | 3848,3,143 |
| 3850,1 | 3851,2,392 | 3852,1 | 3853,6,96 | 3856,3,1042 | 3859,14,1873 | 3861,7,1745 | 3862,11,544 | 3864,5,548 | 3867,7,1329 |
| 3868,9,1177 | 3869,3,621 | 3872,3,516 | 3874,7,372 | 3875,2,533 | 3876,1 | 3877,6,1504 | 3878,2,641 | 3880,3,316 | 3883,13,39 |
| 3885,3,631 | 3888,2,73 | 3890,3,353 | 3891,2,46 | 3893,3,713 | 3896,8,1179 | 3898,3,1060 | 3899,2,845 | 3901,3,1453 | 3904,3,621 |
| 3906,1 | 3907,7,311 | 3909,3,317 | 3910,5,1211 | 3912,2,217 | 3915,14,57 | 3916,1 | 3917,8,1206 | 3920,3,282 | 3922,1 |
| 3923,2,1154 | 3925,14,758 | 3926,2,275 | 3928,3,96 | 3930,1 | 3931,9,1079 | 3933,5,1533 | 3934,7,563 | 3935,4,497 | 3936,3,1744 |
| 3939,2,1360 | 3940,4,1181 | 3941,6,528 | 3944,2,797 | 3946,1 | 3947,2,1259 | 3949,3,495 | 3952,22,1847 | 3955,8,1408 | 3957,8,1314 |
| 3958,5,370 | 3960,2,421 | 3963,2,166 | 3965,6,960 | 3968,3,1329 | 3971,7,899 | 3973,12,1588 | 3976,3,939 | 3978,3,1201 | 3979,8,737 |
| 3980,5,1343 | 3981,14,1567 | 3982,4,269 | 3984,3,355 | 3986,3,485 | 3987,2,55 | 3988,1 | 3989,3,167 | 3992,3,1397 | 3994,11,44 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3995,2,1565 | 3997,3,57 | 4000,5,1448 | 4002,1 | 4003,5,1495 | 4005,5,1171 | 4006,5,569 | 4008,9,270 | 4010,3,1959 | 4011,2,91 |
| 4012,1 | 4013,3,11 | 4016,5,130 | 4018,1 | 4019,2,398 | 4020,1 | 4021,3,1843 | 4022,2,941 | 4024,18,627 | 4026,3,775 |
| 4027,3,1747 | 4028,5,362 | 4029,6,2006 | 4032,2,1453 | 4035,2,457 | 4037,3,59 | 4040,2,341 | 4042,3,249 | 4043,2,896 | 4045,6,160 |
| 4048,3,1170 | 4051,13,1131 | 4053,8,1565 | 4056,2,817 | 4059,2,406 | 4061,3,741 | 4064,2,1457 | 4067,2,278 | 4069,3,837 | 4072,3,1242 |
| 4075,3,475 | 4076,2,443 | 4077,3,1019 | 4078,11,1082 | 4080,3,1273 | 4082,3,992 | 4083,2,466 | 4085,5,1763 | 4088,2,77 | 4090,1 |
| 4091,2,380 | 4092,1 | 4093,8,469 | 4096,3,600 | 4098,1 | 4099,7,2011 | 4101,3,1049 | 4104,5,1887 | 4107,2,1387 | 4109,8,2037 |
| 4110,2,1069 | 4112,7,22 | 4115,2,998 | 4117,3,489 | 4118,4,1141 | 4120,7,1843 | 4121,2,236 | 4123,3,183 | 4128,2,349 | 4130,3,65 |
| 4131,2,1966 | 4132,1 | 4133,16,1438 | 4136,2,1733 | 4138,1 | 4139,2,1808 | 4141,7,2001 | 4144,3,1401 | 4147,18,1966 | 4149,3,857 |
| 4152,3,47 | 4153,5,1103 | 4155,2,1246 | 4156,1 | 4157,3,153 | 4160,3,1835 | 4163,2,1067 | 4165,6,1200 | 4168,3,310 | 4171,10,475 |
| 4172,5,1982 | 4173,3,797 | 4176,2,1597 | 4178,3,405 | 4179,3,2059 | 4181,8,81 | 4184,14,1699 | 4187,2,902 | 4189,5,1061 | 4190,7,388 |
| 4192,3,139 | 4194,3,593 | 4195,5,83 | 4197,5,1577 | 4198,7,72 | 4200,3,442 | 4203,2,268 | 4205,11,375 | 4208,3,461 | 4211,2,1706 |
| 4213,3,1735 | 4216,3,435 | 4218,1 | 4219,7,659 | 4221,5,2021 | 4222,8,461 | 4224,2,2077 | 4226,3,1424 | 4227,2,853 | 4228,1 |
| 4229,3,1175 | 4232,7,692 | 4235,2,224 | 4237,6,1299 | 4240,5,2113 | 4242,1 | 4243,8,589 | 4245,6,1706 | 4248,2,1 | 4250,3,1650 |
| 4251,2,226 | 4252,1 | 4253,8,1806 | 4254,2,1 | 4256,3,1457 | 4258,1 | 4259,2,47 | 4260,1 | 4261,3,339 | 4264,3,2106 |
| 4267,9,1475 | 4269,3,1357 | 4270,5,212 | 4272,3,218 | 4275,2,1150 | 4277,5,1163 | 4280,3,942 | 4282,1 | 4283,2,524 | 4285,10,1343 |
| 4286,2,581 | 4288,7,1444 | 4291,11,23 | 4292,4,2113 | 4293,3,365 | 4294,9,982 | 4296,3,1468 | 4297,12,234 | 4298,3,1674 | 4299,2,1414 |
| 4301,8,835 | 4304,2,1829 | 4306,9,609 | 4307,2,44 | 4309,5,401 | 4310,5,549 | 4312,3,99 | 4315,13,375 | 4317,16,1745 | 4320,2,157 |
| 4323,2,1891 | 4325,3,269 | 4328,3,459 | 4331,2,671 | 4333,10,1590 | 4334,2,2111 | 4336,3,2025 | 4339,3,1291 | 4341,10,2153 | 4344,7,1031 |
| 4347,2,607 | 4348,1 | 4349,8,648 | 4352,7,1457 | 4354,3,162 | 4355,2,1229 | 4356,1 | 4357,6,372 | 4360,3,1354 | 4362,1 |
| 4363,8,916 | 4365,6,1390 | 4368,2,613 | 4370,3,1569 | 4371,2,94 | 4372,1 | 4373,3,243 | 4376,3,1868 | 4379,5,477 | 4381,6,1875 |
| 4384,3,60 | 4385,2,1595 | 4387,3,2091 | 4388,4,41 | 4389,16,1034 | 4392,3,382 | 4393,4,399 | 4395,3,871 | 4396,1 | 4397,7,1097 |
| 4400,2,689 | 4403,2,1502 | 4405,3,1089 | 4407,4,672 | 4408,7,1717 | 4411,3,1279 | 4413,5,535 | 4414,5,4 | 4416,2,1213 | 4418,3,230 |
| 4419,2,1327 | 4421,6,104 | 4424,2,1409 | 4426,3,1299 | 4427,2,1760 | 4429,7,1183 | 4430,5,1729 | 4432,3,447 | 4435,9,1517 | 4437,3,479 |
| 4438,16,523 | 4440,2,661 | 4443,2,2068 | 4448,2,1853 | 4450,1 | 4451,2,107 | 4453,3,1447 | 4456,27,916 | 4459,13,685 | 4461,3,1009 |
| 4462,5,442 | 4464,3,152 | 4467,2,853 | 4469,3,641 | 4472,3,146 | 4475,2,452 | 4477,6,1588 | 4478,2,1301 | 4480,3,660 | 4482,1 |
| 4483,8,1906 | 4485,3,1165 | 4488,3,209 | 4491,11,1133 | 4492,1 | 4493,3,2057 | 4496,2,665 | 4498,10,961 | 4499,2,1415 | 4501,8,149 |
| 4503,4,279 | 4504,3,214 | 4506,1 | 4507,7,979 | 4509,10,961 | 4510,5,1201 | 4512,2,301 | 4515,5,171 | 4516,1 | 4517,3,459 |
| 4520,3,1020 | 4523,3,615 | 4525,3,373 | 4528,3,384 | 4531,10,130 | 4532,2,1451 | 4533,15,431 | 4536,3,281 | 4539,2,352 | 4541,3,227 |
| 4544,2,1673 | 4546,1 | 4547,2,1160 | 4549,3,1399 | 4552,7,1098 | 4555,9,1973 | 4556,5,1559 | 4560,2,1729 | 4563,2,1009 | 4565,3,1055 |
| 4568,5,691 | 4571,2,644 | 4573,3,645 | 4576,3,1809 | 4577,2,545 | 4579,10,979 | 4580,2,323 | 4581,3,569 | 4582,5,575 | 4584,5,204 |
| 4587,2,1864 | 4589,5,395 | 4592,2,1433 | 4593,2,1384 | 4594,3,2059 | 4595,2,824 | 4597,10,815 | 4598,7,164 | 4600,3,1392 | 4602,1 |
| 4603,7,1653 | 4605,3,17 | 4608,3,200 | 4611,7,695 | 4613,5,1835 | 4616,3,1311 | 4619,2,371 | 4620,1 | 4621,3,439 | 4622,2,983 |
| 4624,7,1387 | 4627,12,1989 | 4629,10,1238 | 4630,5,428 | 4631,5,125 | 4632,2,1081 | 4635,3,1007 | 4636,1 | 4637,9,2175 | 4638,5,432 |
| 4640,3,279 | 4643,2,662 | 4645,12,1607 | 4646,2,2291 | 4648,3,1989 | 4651,7,771 | 4653,3,409 | 4654,9,727 | 4656,7,997 | 4659,2,808 |
| 4661,6,1668 | 4664,2,2201 | 4666,6,2029 | 4667,2,362 | 4669,3,2073 | 4670,4,497 | 4672,5,1250 | 4674,7,694 | 4675,3,703 | 4677,3,1447 |
| 4680,10,125 | 4683,2,631 | 4685,3,603 | 4688,2,1037 | 4690,1 | 4691,2,1109 | 4693,3,121 | 4696,3,1434 | 4699,9,757 | 4701,7,1157 |
| 4702,4,1589 | 4704,2,313 | 4707,10,630 | 4709,3,941 | 4712,3,839 | 4714,3,457 | 4715,2,638 | 4717,3,657 | 4718,2,53 | 4720,3,1842 |
| 4721,2,1421 | 4722,1 | 4723,8,395 | 4725,7,1055 | 4728,2,1633 | 4730,3,131 | 4731,5,591 | 4733,5,1485 | 4736,12,1717 | 4738,3,727 |
| 4739,2,170 | 4741,8,1426 | 4744,3,1146 | 4747,10,1025 | 4749,3,347 | 4752,3,1543 | 4755,2,925 | 4757,7,307 | 4760,2,509 | 4762,3,1219 |
| 4763,2,632 | 4765,3,523 | 4766,2,1691 | 4768,5,476 | 4771,5,319 | 4773,10,1643 | 4774,10,2289 | 4776,3,946 | 4778,17,547 | 4779,3,103 |
| 4781,3,827 | 4784,3,1488 | 4786,1 | 4787,2,191 | 4788,1 | 4789,3,1041 | 4792,7,2336 | 4794,6,317 | 4795,3,1899 | 4796,5,1514 |
| 4797,6,496 | 4800,3,1375 | 4803,2,1201 | 4804,4,617 | 4808,5,1212 | 4811,2,548 | 4812,1 | 4813,15,303 | 4814,2,233 | 4816,11,1453 |
| 4819,12,1113 | 4821,3,1895 | 4822,9,1827 | 4824,2,13 | 4826,3,1950 | 4827,2,523 | 4829,3,1175 | 4832,5,664 | 4834,10,277 | 4835,2,269 |
| 4837,13,2151 | 4838,4,1841 | 4840,3,1089 | 4841,2,161 | 4842,4,79 | 4843,5,1003 | 4844,2,1247 | 4845,22,1954 | 4848,6,591 | 4851,2,1975 |
| 4853,3,15 | 4856,2,797 | 4859,2,1202 | 4861,10,1458 | 4862,2,215 | 4864,3,559 | 4866,3,754 | 4867,5,845 | 4869,6,2351 | 4872,2,2401 |
| 4875,2,670 | 4876,1 | 4877,3,269 | 4880,2,1721 | 4882,3,1794 | 4883,2,1322 | 4885,3,811 | 4888,9,234 | 4891,11,1613 | 4893,5,1999 |
| 4896,2,637 | 4898,3,248 | 4899,2,1663 | 4901,3,509 | 4904,5,1150 | 4906,3,510 | 4907,20,185 | 4909,3,715 | 4912,3,1438 | 4915,9,1931 |
| 4917,3,1033 | 4920,2,1693 | 4923,2,1486 | 4925,5,949 | 4928,16,1379 | 4931,2,485 | 4932,1 | 4933,8,2215 | 4936,3,2203 | 4938,3,200 |
| 4939,18,2474 | 4941,5,1425 | 4942,7,1194 | 4944,2,1597 | 4946,7,1084 | 4947,2,775 | 4949,3,785 | 4952,2,797 | 4954,3,276 | 4955,2,905 |
| 4956,1 | 4957,3,2169 | 4960,7,1643 | 4962,3,346 | 4963,3,1135 | 4964,5,956 | 4965,3,235 | 4968,3,157 | 4971,2,208 | 4972,1 |
| 4973,5,1089 | 4976,2,1649 | 4979,2,359 | 4981,6,2092 | 4984,3,435 | 4986,1 | 4987,3,627 | 4989,5,749 | 4990,4,1053 | 4992,3,1973 |
| 4995,2,556 | 4996,10,1305 | 4997,7,1537 | 4999,13,433 | 5000,3,834 | 5002,1 | 5003,2,8 | 5005,3,583 | 5006,2,1175 | 5008,3,1633 |
| 5010,1 | 5011,3,1371 | 5013,9,1295 | 5016,2,1333 | 5019,3,163 | 5021,6,1635 | 5024,3,1137 | 5026,3,2424 | 5027,2,272 | 5029,5,1 |
| 5032,7,1165 | 5035,3,2479 | 5037,5,55 | 5040,2,925 | 5043,3,1691 | 5045,3,465 | 5046,2,2179 | 5048,3,341 | 5050,1 | 5051,2,965 |
| 5053,3,1011 | 5056,3,540 | 5058,1 | 5059,12,1700 | 5061,3,695 | 5064,3,949 | 5067,2,139 | 5069,3,2435 | 5070,2,2131 | 5072,2,365 |
| 5075,2,2459 | 5076,1 | 5077,3,1933 | 5080,3,528 | 5083,16,835 | 5085,3,1117 | 5086,5,140 | 5088,2,757 | 5091,2,556 | 5093,5,143 |
| 5096,11,1926 | 5098,1 | 5099,2,1202 | 5101,8,913 | 5102,2,2225 | 5104,3,957 | 5106,1 | 5107,5,113 | 5109,5,775 | 5112,2,2149 |
| 5115,2,883 | 5117,5,1103 | 5120,3,2195 | 5123,5,745 | 5125,12,571 | 5126,5,487 | 5128,7,1387 | 5131,16,230 | 5133,7,2093 | 5136,3,313 |
| 5139,2,637 | 5141,14,819 | 5142,5,2189 | 5144,2,1961 | 5146,1 | 5147,2,1841 | 5149,6,1776 | 5152,3,253 | 5154,3,1009 | 5155,3,823 |
| 5156,5,1739 | 5157,3,1853 | 5158,5,647 | 5160,5,1289 | 5163,2,1336 | 5164,4,2241 | 5165,5,1869 | 5168,3,911 | 5170,1 | 5171,2,635 |
| 5173,3,51 | 5176,3,690 | 5178,1 | 5179,7,369 | 5181,3,1153 | 5182,4,2189 | 5184,5,2357 | 5187,2,946 | 5188,1 | 5189,8,2485 |
| 5192,2,1073 | 5194,3,36 | 5195,2,740 | 5197,3,1479 | 5198,7,1123 | 5200,3,181 | 5203,3,2559 | 5205,10,1409 | 5208,3,1037 | 5211,2,1102 |
| 5213,3,1403 | 5214,2,1579 | 5216,2,173 | 5219,2,1235 | 5221,11,745 | 5224,7,778 | 5226,1 | 5227,3,3 | 5229,3,1003 | 5230,5,668 |
| 5232,5,146 | 5235,2,652 | 5237,3,363 | 5240,2,1541 | 5243,2,1688 | 5245,5,353 | 5248,13,291 | 5251,13,887 | 5253,5,1961 | 5256,3,1060 |
| 5259,2,1324 | 5260,1 | 5261,7,2309 | 5262,2,1549 | 5264,3,855 | 5267,2,2117 | 5269,3,2131 | 5272,3,873 | 5274,3,737 | 5275,5,2569 |
| 5277,3,983 | 5280,2,253 | 5281,10,2011 | 5282,5,815 | 5283,2,1642 | 5284,9,924 | 5285,3,219 | 5286,2,277 | 5288,3,2529 | 5290,3,1804 |
| 5291,2,1463 | 5293,3,691 | 5294,2,11 | 5296,7,472 | 5299,5,553 | 5301,3,2059 | 5304,2,769 | 5306,3,765 | 5307,2,2497 | 5308,1 |
| 5309,8,63 | 5312,2,305 | 5315,2,218 | 5317,16,1608 | 5320,3,856 | 5323,8,1045 | 5325,3,2495 | 5328,3,439 | 5331,2,313 | 5332,1 |
| 5333,6,2498 | 5335,3,1209 | 5336,2,617 | 5339,2,221 | 5341,5,2329 | 5342,2,1175 | 5344,7,72 | 5347,5,415 | 5349,3,383 | 5350,5,1508 |
| 5352,2,1933 | 5354,3,3 | 5355,3,415 | 5357,7,1277 | 5360,3,528 | 5362,3,849 | 5363,2,1673 | 5365,12,346 | 5366,5,546 | 5368,5,1978 |
| 5371,5,107 | 5373,40,2272 | 5374,4,1821 | 5376,2,1801 | 5379,2,49 | 5381,5,693 | 5382,2,235 | 5384,2,5 | 5386,1 | 5387,2,2357 |
| 5389,3,195 | 5392,3,648 | 5395,22,896 | 5397,3,317 | 5400,5,783 | 5402,3,2628 | 5403,9,1241 | 5405,7,521 | 5408,10,661 | 5411,2,1625 |
| 5413,8,826 | 5414,2,371 | 5416,3,129 | 5419,3,1447 | 5421,3,905 | 5424,3,1508 | 5426,5,1724 | 5427,2,373 | 5429,18,254 | 5432,5,457 |
| 5434,3,183 | 5435,2,1682 | 5437,3,367 | 5440,3,2547 | 5442,1 | 5443,5,431 | 5445,7,2687 | 5448,2,121 | 5451,2,934 | 5453,3,1325 |
| 5456,2,1157 | 5459,2,1346 | 5461,7,247 | 5462,5,1252 | 5464,5,2450 | 5466,3,1924 | 5467,3,2451 | 5469,6,1553 | 5470,5,1208 | 5472,2,2509 |
| 5475,2,949 | 5476,1 | 5477,3,1439 | 5480,2,533 | 5482,1 | 5483,3,2531 | 5485,5,2317 | 5486,5,262 | 5488,3,996 | 5491,9,509 |
| 5493,3,311 | 5496,5,2304 | 5498,3,681 | 5499,2,784 | 5500,1 | 5501,3,1865 | 5504,2,1757 | 5506,1 | 5507,2,431 | 5509,6,2649 |
| 5510,2,2741 | 5512,3,2328 | 5515,3,115 | 5517,19,1347 | 5518,5,1496 | 5520,9,723 | 5522,3,1539 | 5523,2,166 | 5525,3,743 | 5528,3,752 |
| 5531,9,2449 | 5533,3,1731 | 5536,5,59 | 5538,3,706 | 5539,5,59 | 5541,5,1989 | 5544,2,949 | 5546,3,246 | 5547,2,700 | 5549,14,1140 |
| 5552,2,761 | 5554,3,1731 | 5555,2,806 | 5556,1 | 5557,3,199 | 5560,3,1660 | 5562,1 | 5563,11,1351 | 5565,3,37 | 5568,3,536 |
| 5570,3,2033 | 5571,2,1630 | 5572,1 | 5573,3,2169 | 5576,6,251 | 5578,3,1126 | 5579,2,413 | 5581,13,1939 | 5584,3,612 | 5587,9,2057 |
| 5589,3,2279 | 5592,2,1021 | 5595,2,1285 | 5597,8,882 | 5600,9,2716 | 5603,7,521 | 5605,9,2031 | 5608,3,1630 | 5611,5,2137 | 5613,3,2537 |
| 5614,4,1277 | 5616,2,1345 | 5618,5,1889 | 5619,2,94 | 5621,5,1163 | 5624,3,996 | 5627,2,632 | 5629,3,1945 | 5632,5,2788 | 5635,5,1913 |
| 5637,8,2219 | 5638,5,727 | 5640,2,1621 | 5642,31,1775 | 5643,2,1903 | 5645,5,121 | 5646,7,2640 | 5647,4,2069 | 5648,3,129 | 5650,1 |
| 5651,2,233 | 5653,13,273 | 5656,5,2240 | 5658,1 | 5659,3,2347 | 5661,3,1081 | 5664,5,1067 | 5667,2,2422 | 5668,4,653 | 5669,3,2775 |
| 5672,3,2528 | 5674,6,139 | 5675,2,1931 | 5677,11,1831 | 5678,2,311 | 5680,3,618 | 5682,1 | 5683,3,2551 | 5685,3,1111 | 5686,10,1011 |
| 5688,6,1663 | 5691,2,292 | 5692,1 | 5693,3,165 | 5696,3,68 | 5697,2,1225 | 5698,3,247 | 5699,2,1841 | 5700,1 | 5701,3,1635 |
| 5702,2,1001 | 5704,3,220 | 5707,9,1289 | 5709,5,619 | 5712,3,2423 | 5715,2,685 | 5716,1 | 5717,6,1955 | 5720,2,1901 | 5722,3,1563 |
| 5723,2,1232 | 5725,3,633 | 5728,3,928 | 5730,5,2386 | 5731,3,619 | 5733,9,1121 | 5736,2,1801 | 5738,3,360 | 5739,2,2107 | 5740,1 |
| 5741,11,573 | 5744,5,142 | 5747,2,653 | 5748,1 | 5749,18,1432 | 5752,3,31 | 5755,5,2453 | 5757,6,46 | 5760,2,2209 | 5763,2,109 |
| 5765,7,2771 | 5766,2,1045 | 5768,2,1709 | 5770,4,2163 | 5771,2,356 | 5773,6,2347 | 5774,2,1973 | 5776,3,628 | 5778,1 | 5779,10,248 |
| 5781,3,1511 | 5784,2,409 | 5786,8,2475 | 5787,2,1006 | 5789,3,2837 | 5792,3,2249 | 5795,2,2417 | 5797,3,1749 | 5800,5,1307 | 5803,5,1615 |
| 5804,5,179 | 5805,7,493 | 5808,2,1777 | 5811,2,1831 | 5812,1 | 5813,8,2331 | 5816,3,216 | 5821,6,1279 | 5824,3,2836 | 5826,1 |
| 5827,7,2609 | 5828,5,1994 | 5829,7,1367 | 5830,4,1713 | 5832,2,1189 | 5835,2,82 | 5837,3,2211 | 5840,2,2717 | 5842,1 | 5843,3,1851 |
| 5845,3,2865 | 5846,9,2758 | 5848,3,303 | 5850,1 | 5851,5,581 | 5852,7,2311 | 5853,7,911 | 5856,5,842 | 5859,2,1360 | 5861,7,2579 |
| 5862,2,769 | 5864,2,2405 | 5866,3,2130 | 5867,2,503 | 5868,1 | 5869,3,205 | 5870,2,2609 | 5872,3,2761 | 5875,18,2910 | 5877,6,1322 |
| 5878,7,1854 | 5880,2,1261 | 5883,2,604 | 5884,4,231 | 5885,13,1823 | 5888,3,1958 | 5890,7,691 | 5891,2,269 | 5893,8,55 | 5894,10,1483 |
| 5896,6,1803 | 5899,5,2245 | 5901,5,43 | 5904,2,2389 | 5906,3,54 | 5907,2,1495 | 5909,7,1643 | 5912,12,2327 | 5914,3,787 | 5915,2,218 |
| 5916,3,1973 | 5917,6,466 | 5918,2,713 | 5920,3,1230 | 5922,1 | 5923,7,1269 | 5925,3,1481 | 5928,3,2561 | 5929,9,1547 | 5930,3,2847 |
| 5931,2,1045 | 5933,18,2627 | 5934,2,811 | 5936,3,1919 | 5938,1 | 5939,2,1136 | 5941,7,2451 | 5944,3,573 | 5945,2,1040 | 5946,3,2494 |
| 5947,7,1543 | 5949,3,1445 | 5950,5,2581 | 5952,2,1585 | 5955,2,2743 | 5957,6,1599 | 5960,3,1089 | 5963,2,41 | 5965,3,1287 | 5968,5,823 |
| 5971,9,1253 | 5973,6,2809 | 5974,5,1408 | 5976,2,2029 | 5979,2,250 | 5981,5,815 | 5984,3,6 | 5986,1 | 5987,2,1187 | 5989,7,419 |
| 5992,3,37 | 5994,3,2783 | 5995,3,835 | 5996,8,1215 | 5997,10,12 | 6000,2,2329 | 6003,2,328 | 6005,3,1511 | 6008,3,1163 | 6010,1 |
| 6011,2,254 | 6013,8,1306 | 6014,2,473 | 6016,7,246 | 6019,3,619 | 6021,10,1892 | 6024,5,102 | 6028,1 | 6029,3,921 | 6032,3,551 |
| 6035,2,1427 | 6037,3,919 | 6038,5,925 | 6040,3,990 | 6042,3,1244 | 6043,3,2115 | 6045,5,2513 | 6046,5,1379 | 6048,3,2074 | 6051,2,2527 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 6052,1 | 6053,3,1083 | 6054,2,1471 | 6056,3,264 | 6059,2,647 | 6061,3,493 | 6062,2,641 | 6063,4,328 | 6064,3,1236 | 6066,1 |
| 6067,7,1183 | 6069,11,1373 | 6072,5,855 | 6075,2,1054 | 6077,3,1853 | 6080,2,1097 | 6082,3,1098 | 6083,2,1268 | 6085,3,2829 | 6088,3,880 |
| 6091,3,103 | 6093,6,1670 | 6096,2,457 | 6099,2,112 | 6100,1 | 6101,5,2687 | 6102,4,2517 | 6104,3,135 | 6107,2,1631 | 6109,3,2691 |
| 6110,5,2353 | 6112,3,264 | 6114,3,2293 | 6115,5,541 | 6117,3,2267 | 6120,2,1981 | 6122,5,2768 | 6123,5,1505 | 6125,3,1289 | 6126,5,983 |
| 6127,3,813 | 6128,3,459 | 6130,1 | 6131,14,222 | 6133,3,1503 | 6136,5,1220 | 6138,13,543 | 6139,12,81 | 6141,3,1523 | 6144,2,1501 |
| 6147,2,487 | 6148,4,2889 | 6149,6,1716 | 6152,5,693 | 6154,3,447 | 6155,2,1436 | 6157,6,2260 | 6158,5,1435 | 6160,3,751 | 6163,17,2279 |
| 6165,7,2057 | 6166,7,1625 | 6168,2,2209 | 6171,5,467 | 6172,1 | 6173,5,2265 | 6176,3,1355 | 6179,2,668 | 6181,5,2197 | 6184,3,2403 |
| 6186,3,481 | 6187,5,2593 | 6189,3,629 | 6192,5,1428 | 6194,3,48 | 6195,2,40 | 6196,1 | 6197,3,1103 | 6200,3,1160 | 6202,1 |
| 6203,2,2252 | 6205,3,2641 | 6206,2,1223 | 6208,3,150 | 6210,1 | 6211,5,1405 | 6212,2,947 | 6213,8,1715 | 6216,5,668 | 6219,2,259 |
| 6221,3,969 | 6224,3,1461 | 6227,2,8 | 6228,1 | 6229,3,1987 | 6232,3,312 | 6234,5,202 | 6235,10,2057 | 6237,3,29 | 6240,2,961 |
| 6242,4,2363 | 6243,2,46 | 6245,7,2131 | 6248,11,2650 | 6251,2,1943 | 6252,2,3091 | 6253,3,981 | 6254,5,2020 | 6256,3,1839 | 6259,13,913 |
| 6261,3,599 | 6264,2,685 | 6266,5,935 | 6267,5,605 | 6268,1 | 6269,6,3126 | 6272,2,1517 | 6275,2,2432 | 6276,1 | 6277,6,85 |
| 6280,3,1077 | 6283,13,91 | 6284,4,929 | 6285,3,881 | 6288,2,757 | 6291,2,1933 | 6293,5,597 | 6296,5,879 | 6298,1 | 6299,7,157 |
| 6301,17,491 | 6304,22,2299 | 6307,15,463 | 6309,3,2675 | 6310,5,1618 | 6312,3,1396 | 6314,3,617 | 6315,2,1201 | 6316,1 | 6317,3,2783 |
| 6320,3,342 | 6322,1 | 6323,2,548 | 6325,6,1383 | 6327,4,462 | 6328,3,1408 | 6329,2,635 | 6331,5,1241 | 6333,5,993 | 6336,5,540 |
| 6339,2,1672 | 6341,10,776 | 6344,2,2237 | 6346,6,1237 | 6347,14,876 | 6349,3,757 | 6350,2,461 | 6352,3,487 | 6355,3,2719 | 6357,3,859 |
| 6360,2,2269 | 6361,11,475 | 6363,5,1115 | 6365,3,365 | 6368,2,2921 | 6369,4,711 | 6371,2,791 | 6372,1 | 6373,3,1003 | 6374,2,2387 |
| 6376,3,1354 | 6378,1 | 6379,3,547 | 6381,7,1619 | 6384,2,1285 | 6387,7,1813 | 6388,1 | 6389,3,311 | 6392,5,721 | 6395,2,782 |
| 6396,1 | 6397,3,619 | 6398,5,1633 | 6400,3,102 | 6403,18,1726 | 6405,3,2815 | 6408,2,1609 | 6410,3,1109 | 6411,2,988 | 6413,3,1581 |
| 6414,4,2001 | 6416,2,341 | 6419,2,2006 | 6421,3,1737 | 6423,4,1464 | 6424,3,2572 | 6427,5,409 | 6429,7,929 | 6432,3,1214 | 6435,2,310 |
| 6437,6,2939 | 6440,2,1121 | 6442,3,1047 | 6443,10,3130 | 6445,3,829 | 6448,3,1027 | 6451,8,1375 | 6453,3,2411 | 6456,3,1303 | 6459,2,1726 |
| 6461,3,1905 | 6462,4,2929 | 6464,5,2815 | 6466,3,990 | 6467,2,1859 | 6468,1 | 6469,3,867 | 6472,5,1793 | 6475,3,3207 | 6477,5,2705 |
| 6480,3,1496 | 6482,3,1773 | 6483,2,136 | 6485,14,2636 | 6486,2,2917 | 6488,2,2741 | 6490,1 | 6491,2,542 | 6493,5,61 | 6494,2,3053 |
| 6496,3,3165 | 6499,7,2367 | 6501,5,547 | 6504,2,2257 | 6506,3,410 | 6507,2,154 | 6508,11,20 | 6509,3,1277 | 6512,5,1366 | 6515,2,1529 |
| 6516,5,811 | 6517,5,2345 | 6520,3,1395 | 6523,16,1375 | 6525,7,73 | 6528,2,2401 | 6530,3,164 | 6531,2,949 | 6532,9,538 | 6533,3,1173 |
| 6536,2,2969 | 6539,2,776 | 6541,11,3175 | 6542,2,2327 | 6543,3,997 | 6544,3,2110 | 6546,1 | 6547,11,421 | 6549,5,105 | 6552,2,1201 |
| 6555,2,700 | 6557,7,2507 | 6560,9,34 | 6563,2,1091 | 6565,3,241 | 6566,2,305 | 6568,3,2608 | 6571,3,2271 | 6572,5,2693 | 6573,5,1385 |
| 6574,5,1076 | 6576,3,1019 | 6579,2,214 | 6581,7,2789 | 6582,2,2095 | 6584,5,1222 | 6586,3,1434 | 6587,11,1417 | 6589,3,2857 | 6592,3,969 |
| 6595,8,2191 | 6597,7,1863 | 6600,3,1060 | 6602,3,1014 | 6603,2,2083 | 6605,16,626 | 6608,3,771 | 6610,3,1324 | 6611,2,503 | 6613,8,734 |
| 6616,3,3036 | 6618,1 | 6619,5,1213 | 6621,3,671 | 6624,9,2091 | 6626,5,815 | 6627,2,1594 | 6629,3,1331 | 6632,2,1493 | 6635,2,1163 |
| 6636,1 | 6637,9,2755 | 6640,5,364 | 6643,3,1863 | 6645,8,3003 | 6646,9,119 | 6648,3,1144 | 6651,2,406 | 6652,1 | 6653,3,1815 |
| 6656,3,276 | 6658,1 | 6659,2,893 | 6661,5,1537 | 6664,5,583 | 6667,3,291 | 6669,6,1667 | 6672,3,482 | 6675,2,1879 | 6677,3,2897 |
| 6680,3,956 | 6682,6,2581 | 6683,2,1103 | 6685,6,1711 | 6688,5,2345 | 6690,1 | 6691,8,155 | 6693,3,1637 | 6696,6,111 | 6698,3,1329 |
| 6699,2,568 | 6700,1 | 6701,3,2339 | 6704,2,2441 | 6707,2,1355 | 6708,1 | 6709,3,2193 | 6712,5,4 | 6715,16,209 | 6717,7,1865 |
| 6718,5,2497 | 6720,3,3221 | 6723,2,2278 | 6725,3,2441 | 6728,3,2750 | 6731,2,365 | 6732,1 | 6733,6,325 | 6734,5,819 | 6736,3,403 |
| 6738,11,462 | 6739,3,243 | 6741,3,1219 | 6742,7,1799 | 6744,3,3173 | 6747,2,2263 | 6749,3,2015 | 6752,2,5 | 6755,2,635 | 6760,3,1846 |
| 6762,1 | 6763,5,355 | 6765,6,635 | 6766,5,637 | 6768,2,1009 | 6770,7,871 | 6771,2,946 | 6773,6,755 | 6776,3,29 | 6778,1 |
| 6779,2,875 | 6780,1 | 6781,3,75 | 6784,7,1822 | 6787,15,2515 | 6789,5,2849 | 6790,5,2558 | 6792,2,2065 | 6795,2,2284 | 6797,3,989 |
| 6800,5,1327 | 6802,1 | 6803,2,1037 | 6805,8,1367 | 6806,2,77 | 6808,15,1308 | 6809,4,214 | 6811,5,1777 | 6813,3,155 | 6814,5,3175 |
| 6816,3,551 | 6819,2,661 | 6821,5,1475 | 6823,3,1573 | 6824,3,1413 | 6826,1 | 6827,14,307 | 6828,1 | 6829,5,2149 | 6832,3,499 |
| 6834,3,1303 | 6835,3,2935 | 6837,7,2327 | 6840,2,2533 | 6842,3,1691 | 6843,7,133 | 6844,7,488 | 6845,2,2 | 6848,2,533 | 6850,6,1839 |
| 6851,2,881 | 6853,3,2977 | 6854,2,1295 | 6856,3,709 | 6859,3,31 | 6861,5,1747 | 6864,2,2569 | 6867,2,2104 | 6868,1 | 6869,3,81 |
| 6870,12,1469 | 6872,2,185 | 6875,2,761 | 6877,3,2517 | 6878,4,721 | 6879,4,1027 | 6880,3,811 | 6882,1 | 6883,5,1193 | 6885,6,1889 |
| 6888,3,394 | 6890,9,374 | 6891,2,1948 | 6893,3,411 | 6894,4,3157 | 6896,5,1756 | 6897,10,3431 | 6898,1 | 6899,2,797 | 6901,3,825 |
| 6904,5,409 | 6906,1 | 6907,13,1949 | 6909,3,1955 | 6912,2,1669 | 6914,3,1251 | 6915,2,1693 | 6916,1 | 6917,8,1701 | 6919,4,1787 |
| 6920,5,2896 | 6922,3,1938 | 6923,2,1463 | 6925,10,2076 | 6926,2,3143 | 6928,3,691 | 6931,5,491 | 6933,3,1409 | 6934,5,3371 | 6936,2,3397 |
| 6939,2,793 | 6941,5,1907 | 6944,2,1625 | 6945,2,2107 | 6946,1 | 6947,2,2144 | 6948,1 | 6949,3,691 | 6950,2,155 | 6952,3,1966 |
| 6955,5,611 | 6957,5,475 | 6960,3,1135 | 6962,4,1243 | 6963,2,187 | 6965,6,3356 | 6968,3,555 | 6970,1 | 6971,2,1763 | 6973,7,2797 |
| 6976,5,1999 | 6978,3,349 | 6979,13,823 | 6981,3,823 | 6982,4,449 | 6984,3,3190 | 6987,2,3217 | 6989,3,905 | 6992,7,3397 | 6994,4,231 |
| 6995,2,683 | 6997,15,503 | 7000,7,2740 | 7003,3,975 | 7005,3,1013 | 7008,2,229 | 7010,3,1437 | 7011,2,619 | 7012,1 | 7013,3,3195 |
| 7016,3,1572 | 7018,1 | 7019,2,2180 | 7021,3,3025 | 7024,3,3322 | 7026,1 | 7027,7,2157 | 7028,5,1709 | 7029,3,1385 | 7032,2,313 |
| 7035,2,151 | 7037,3,2297 | 7040,5,2 | 7042,1 | 7043,2,1343 | 7045,5,869 | 7048,3,160 | 7051,3,1243 | 7053,14,1419 | 7054,5,161 |
| 7056,3,380 | 7059,2,535 | 7061,3,1655 | 7064,3,1308 | 7066,9,2226 | 7067,2,365 | 7068,1 | 7069,6,1374 | 7072,3,3417 | 7075,8,2236 |
| 7078,7,1407 | 7080,2,2137 | 7083,2,172 | 7085,4,2 | 7086,5,3515 | 7088,2,1673 | 7090,3,913 | 7091,2,1748 | 7093,3,1345 | 7094,4,809 |
| 7096,3,292 | 7099,3,391 | 7101,5,103 | 7102,10,2577 | 7104,2,1189 | 7107,2,175 | 7108,1 | 7109,12,3334 | 7112,3,3348 | 7114,3,687 |
| 7115,2,1220 | 7117,3,1879 | 7120,3,964 | 7122,3,2314 | 7123,11,2431 | 7125,8,1758 | 7128,2,757 | 7130,5,2854 | 7131,2,1504 | 7133,10,2626 |
| 7136,3,1052 | 7138,3,789 | 7139,8,2629 | 7141,20,1115 | 7142,4,2953 | 7144,9,3065 | 7147,7,3509 | 7149,14,1840 | 7152,3,2978 | 7154,15,45 |
| 7155,2,532 | 7157,3,1857 | 7158,2,2527 | 7160,7,571 | 7163,2,1886 | 7165,10,502 | 7168,3,576 | 7171,5,737 | 7173,5,835 | 7174,9,476 |
| 7176,2,1693 | 7178,4,971 | 7179,2,325 | 7181,5,3073 | 7184,3,221 | 7186,1 | 7187,2,506 | 7188,4,789 | 7189,3,2479 | 7192,5,2080 |
| 7195,8,16 | 7197,3,209 | 7198,5,1972 | 7200,6,739 | 7205,5,789 | 7208,5,418 | 7210,1 | 7211,2,3035 | 7212,2,2215 | 7213,3,2011 |
| 7214,8,1347 | 7216,3,412 | 7218,1 | 7219,3,1975 | 7221,7,951 | 7224,2,2893 | 7227,2,1000 | 7228,1 | 7229,3,1641 | 7232,3,411 |
| 7234,3,3196 | 7235,2,122 | 7236,1 | 7237,3,307 | 7238,7,1327 | 7240,3,169 | 7242,1 | 7243,9,3611 | 7245,3,2165 | 7248,3,1829 |
| 7251,2,967 | 7252,1 | 7253,9,409 | 7256,5,3040 | 7259,3,1115 | 7261,3,81 | 7262,2,2537 | 7264,7,142 | 7267,3,1287 | 7268,4,3031 |
| 7269,3,2123 | 7272,3,437 | 7274,3,335 | 7275,7,877 | 7277,5,873 | 7280,2,3329 | 7282,1 | 7283,2,1967 | 7285,10,307 | 7288,3,495 |
| 7291,5,2851 | 7293,8,1052 | 7294,5,1501 | 7296,3,179 | 7298,8,1055 | 7299,2,1228 | 7301,11,1407 | 7304,3,2531 | 7306,1 | 7307,2,1478 |
| 7309,3,1867 | 7312,7,1390 | 7315,7,1049 | 7317,3,743 | 7320,2,1849 | 7323,2,49 | 7325,6,1145 | 7328,3,1028 | 7330,1 | 7331,2,287 |
| 7333,18,376 | 7336,3,1759 | 7339,3,751 | 7341,5,2899 | 7344,3,3344 | 7347,5,467 | 7348,1 | 7349,3,1007 | 7352,2,2369 | 7355,2,5 |
| 7357,6,229 | 7358,2,1853 | 7360,3,135 | 7363,8,2246 | 7365,10,2434 | 7368,2,841 | 7371,2,2308 | 7373,8,3006 | 7376,2,1361 | 7379,5,2589 |
| 7381,5,2849 | 7384,3,1315 | 7387,5,2729 | 7389,8,3012 | 7390,5,433 | 7392,9,549 | 7395,2,409 | 7396,8,1331 | 7397,9,2305 | 7400,2,1685 |
| 7403,2,1043 | 7405,6,3457 | 7406,2,2795 | 7407,14,2602 | 7408,3,3375 | 7410,1 | 7411,7,2027 | 7413,9,1841 | 7414,4,3681 | 7415,4,1127 |
| 7416,3,205 | 7419,2,298 | 7420,7,1061 | 7421,15,3565 | 7424,9,3382 | 7427,2,569 | 7429,3,2703 | 7430,2,2123 | 7432,3,3561 | 7435,3,27 |
| 7437,3,1957 | 7440,2,2953 | 7442,3,2001 | 7443,2,1054 | 7445,6,3002 | 7448,2,809 | 7450,1 | 7451,2,2666 | 7453,3,1473 | 7454,5,2605 |
| 7456,5,2590 | 7457,4,2603 | 7458,1 | 7459,8,1435 | 7461,3,1291 | 7464,5,1977 | 7467,3,1979 | 7469,5,3129 | 7470,5,3486 | 7472,3,2144 |
| 7474,3,1426 | 7475,2,35 | 7476,1 | 7477,3,1147 | 7480,5,2002 | 7482,3,1168 | 7483,9,2083 | 7485,3,197 | 7486,5,896 | 7488,2,2029 |
| 7491,2,2119 | 7493,3,1143 | 7494,2,1009 | 7496,3,2894 | 7498,1 | 7499,3,1275 | 7501,10,1912 | 7502,2,671 | 7504,3,562 | 7506,1 |
| 7507,3,3231 | 7509,3,857 | 7510,4,3153 | 7512,3,1699 | 7514,3,1691 | 7515,2,1006 | 7516,1 | 7517,5,83 | 7520,3,2682 | 7522,1 |
| 7523,2,929 | 7525,7,1873 | 7528,3,3007 | 7531,3,3195 | 7533,7,401 | 7536,7,1781 | 7539,3,1339 | 7540,1 | 7541,7,59 | 7544,3,1727 |
| 7546,1 | 7547,2,167 | 7548,1 | 7549,6,1789 | 7550,2,1877 | 7552,3,363 | 7554,3,544 | 7555,10,1996 | 7557,5,2215 | 7560,2,1765 |
| 7563,3,527 | 7565,5,2423 | 7568,3,3540 | 7571,2,1097 | 7572,1 | 7573,3,2743 | 7576,5,2834 | 7579,12,3018 | 7581,3,2549 | 7582,4,1617 |
| 7584,2,229 | 7587,2,1030 | 7588,1 | 7589,3,167 | 7592,2,2297 | 7595,5,751 | 7597,17,859 | 7600,3,990 | 7602,1 | 7603,10,1977 |
| 7605,24,2213 | 7606,5,2179 | 7608,2,3469 | 7610,3,356 | 7611,3,1751 | 7613,5,2221 | 7615,4,1631 | 7616,2,3581 | 7617,2,481 | 7618,3,631 |
| 7619,2,1988 | 7620,1 | 7621,3,775 | 7624,3,1174 | 7627,5,1597 | 7629,3,545 | 7632,2,721 | 7633,4,669 | 7635,2,715 | 7637,3,2277 |
| 7640,3,1584 | 7642,1 | 7643,3,2103 | 7645,3,1105 | 7648,9,3041 | 7651,5,3149 | 7653,3,1415 | 7654,5,365 | 7656,2,97 | 7659,2,3181 |
| 7661,3,1929 | 7664,2,809 | 7667,2,353 | 7668,1 | 7669,6,244 | 7670,2,1259 | 7672,3,946 | 7675,3,3595 | 7676,2,3347 | 7677,3,2203 |
| 7680,3,565 | 7683,2,778 | 7685,6,353 | 7688,2,1157 | 7690,1 | 7691,2,347 | 7693,6,3727 | 7696,3,1129 | 7699,7,2253 | 7701,3,2729 |
| 7704,7,1592 | 7707,2,1687 | 7709,3,1037 | 7712,5,3031 | 7715,5,1041 | 7716,1 | 7717,5,2485 | 7718,2,719 | 7720,3,430 | 7723,5,3271 |
| 7725,7,833 | 7726,10,413 | 7728,2,2269 | 7731,2,3649 | 7733,3,3545 | 7736,3,720 | 7737,2,1327 | 7739,2,491 | 7741,3,129 | 7744,3,2328 |
| 7746,5,3874 | 7747,5,1795 | 7749,5,21 | 7752,3,1789 | 7754,3,992 | 7755,2,1234 | 7756,1 | 7757,3,587 | 7760,10,3389 | 7763,2,299 |
| 7765,3,1849 | 7768,3,1321 | 7771,7,3587 | 7773,10,354 | 7776,2,2641 | 7778,3,608 | 7779,2,763 | 7781,6,257 | 7782,2,547 | 7784,3,498 |
| 7786,3,3147 | 7787,2,1001 | 7788,1 | 7789,9,1957 | 7792,13,818 | 7795,9,423 | 7797,3,3541 | 7798,5,2806 | 7800,3,1856 | 7803,2,823 |
| 7804,4,1517 | 7805,3,953 | 7806,5,1847 | 7808,3,711 | 7811,2,2081 | 7813,12,3239 | 7816,7,467 | 7819,7,1793 | 7821,9,67 | 7824,15,726 |
| 7827,2,922 | 7828,1 | 7829,9,741 | 7832,3,2127 | 7834,3,1308 | 7835,2,899 | 7836,9,1918 | 7837,15,2037 | 7840,3,631 | 7842,3,358 |
| 7843,7,2693 | 7844,4,1439 | 7845,5,1397 | 7846,14,1399 | 7848,9,1689 | 7851,2,799 | 7852,1 | 7853,3,2019 | 7856,2,1925 | 7859,15,715 |
| 7861,8,1414 | 7862,2,3443 | 7864,5,865 | 7867,5,2669 | 7869,3,3869 | 7872,2,2017 | 7875,2,1234 | 7876,1 | 7877,5,1305 | 7879,4,1607 |
| 7880,7,3011 | 7881,2,3100 | 7882,1 | 7883,3,1455 | 7885,3,1633 | 7886,2,3737 | 7888,5,1766 | 7891,5,131 | 7893,5,401 | 7894,4,1821 |
| 7896,3,2150 | 7898,3,2640 | 7899,2,490 | 7900,1 | 7901,20,3754 | 7904,3,2231 | 7906,1 | 7907,2,881 | 7909,3,1669 | 7912,3,1642 |
| 7914,4,427 | 7915,3,691 | 7916,5,3926 | 7917,8,93 | 7918,5,1828 | 7920,2,1273 | 7923,3,1931 | 7925,5,1497 | 7928,14,3587 | 7930,3,1438 |
| 7931,14,3496 | 7932,1 | 7933,3,1597 | 7936,3,1942 | 7939,3,271 | 7941,7,1807 | 7944,2,1105 | 7947,2,2668 | 7948,1 | 7949,5,839 |
| 7950,2,625 | 7952,2,641 | 7954,7,3779 | 7955,2,3353 | 7957,7,1291 | 7960,3,1399 | 7963,5,2275 | 7965,13,2821 | 7968,8,2973 | 7970,9,437 |
| 7971,2,1630 | 7973,3,3761 | 7974,2,1921 | 7976,7,2144 | 7978,3,171 | 7979,2,839 | 7981,3,1125 | 7982,2,959 | 7984,5,1264 | 7986,3,2005 |
| 7987,5,2179 | 7989,3,2633 | 7992,2,3805 | 7995,2,718 | 7997,3,2321 | 8000,3,1235 | 8002,10,839 | 8003,2,1127 | 8005,6,579 | 8008,3,85 |
| 8011,9,3419 | 8013,5,105 | 8016,5,981 | 8018,5,782 | 8019,7,2159 | 8021,3,1161 | 8023,4,804 | 8024,3,599 | 8027,2,2045 | 8029,3,3649 |
| 8031,3,1229 | 8032,3,2571 | 8035,3,423 | 8037,3,181 | 8038,7,1197 | 8040,2,2113 | 8042,3,234 | 8043,2,2437 | 8045,5,1213 | 8048,2,1517 |
| 8050,3,163 | 8051,25,859 | 8052,1 | 8053,3,487 | 8056,3,3324 | 8059,5,1691 | 8061,13,317 | 8064,5,3674 | 8066,7,2194 | 8067,2,208 |
| 8068,1 | 8069,12,2993 | 8072,9,1375 | 8074,3,3621 | 8075,2,2948 | 8077,7,1765 | 8080,3,340 | 8083,8,1217 | 8085,3,751 | 8088,2,1213 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 8091,2,1015 | 8092,1 | 8093,5,2123 | 8096,5,1936 | 8099,2,590 | 8101,6,949 | 8102,2,2189 | 8104,7,178 | 8107,12,1335 | 8109,3,1297 |
| 8112,3,3937 | 8115,3,3935 | 8116,1 | 8117,22,1829 | 8118,5,2463 | 8120,3,3600 | 8122,1 | 8123,3,2207 | 8125,3,3645 | 8126,2,3185 |
| 8128,3,594 | 8131,14,1477 | 8132,2,491 | 8133,3,2771 | 8136,5,516 | 8139,2,2890 | 8141,3,1625 | 8142,5,2112 | 8144,2,3677 | 8146,1 |
| 8147,2,911 | 8149,3,2295 | 8152,5,2284 | 8155,8,2258 | 8157,17,2695 | 8158,5,2527 | 8160,2,2953 | 8163,2,3238 | 8165,3,2111 | 8168,3,3338 |
| 8170,1 | 8171,2,317 | 8173,6,942 | 8174,2,2339 | 8176,3,2683 | 8178,1 | 8179,12,1753 | 8181,3,871 | 8184,2,3301 | 8186,3,3068 |
| 8187,2,1249 | 8189,3,255 | 8192,2,653 | 8195,2,5 | 8197,12,3234 | 8200,3,3105 | 8202,3,2978 | 8203,9,1093 | 8205,3,97 | 8206,5,1622 |
| 8208,5,239 | 8211,2,232 | 8213,10,2284 | 8214,2,103 | 8216,3,143 | 8218,1 | 8219,2,1088 | 8220,1 | 8221,3,2235 | 8224,3,2341 |
| 8227,3,2031 | 8228,9,1031 | 8229,5,727 | 8232,3,1597 | 8235,2,2221 | 8236,1 | 8237,3,3323 | 8238,5,473 | 8240,3,2043 | 8242,1 |
| 8243,2,356 | 8245,7,1103 | 8248,3,2542 | 8249,2,5 | 8251,7,643 | 8253,6,698 | 8256,2,553 | 8259,2,1477 | 8261,3,503 | 8264,5,3159 |
| 8266,3,2218 | 8267,2,1727 | 8268,1 | 8269,5,1961 | 8270,2,3317 | 8272,3,2889 | 8275,7,2697 | 8277,3,781 | 8280,3,1196 | 8283,2,1843 |
| 8285,6,795 | 8288,3,1031 | 8290,1 | 8291,2,1658 | 8292,1 | 8293,3,1531 | 8294,2,3107 | 8296,5,560 | 8298,4,3403 | 8299,5,385 |
| 8301,3,2971 | 8304,3,2815 | 8306,5,1970 | 8307,2,535 | 8308,9,37 | 8309,6,3092 | 8312,3,2573 | 8314,3,850 | 8315,2,1157 | 8317,3,2869 |
| 8318,2,2921 | 8320,7,1198 | 8322,3,1609 | 8323,8,419 | 8325,8,3279 | 8326,5,3112 | 8328,2,2677 | 8331,2,580 | 8333,3,641 | 8336,3,1476 |
| 8338,12,3643 | 8339,2,1592 | 8341,5,1045 | 8344,3,16 | 8346,3,1016 | 8347,5,2107 | 8349,6,421 | 8352,3,3548 | 8355,2,1189 | 8356,6,345 |
| 8357,6,1668 | 8360,3,1226 | 8361,2,4048 | 8362,1 | 8363,2,1103 | 8365,6,985 | 8368,3,3075 | 8369,2,3704 | 8371,3,2019 | 8373,15,3035 |
| 8376,5,1314 | 8379,2,1897 | 8381,3,2409 | 8382,2,517 | 8383,4,3249 | 8384,3,96 | 8386,1 | 8387,2,2000 | 8389,6,1786 | 8392,3,1651 |
| 8394,3,1279 | 8395,5,823 | 8396,2,2219 | 8397,6,2897 | 8400,2,1969 | 8403,2,2158 | 8405,3,2873 | 8406,9,579 | 8408,8,2875 | 8410,3,1318 |
| 8411,2,362 | 8413,3,633 | 8416,3,711 | 8419,5,361 | 8421,5,3403 | 8422,4,929 | 8424,5,3945 | 8427,2,1120 | 8428,1 | 8429,3,1791 |
| 8432,5,933 | 8435,12,273 | 8437,12,236 | 8438,2,1001 | 8440,3,766 | 8442,1 | 8443,3,391 | 8445,3,2627 | 8448,3,3706 | 8450,7,2476 |
| 8451,11,997 | 8452,4,1347 | 8453,14,13 | 8454,2,1171 | 8456,8,2155 | 8458,15,682 | 8459,2,1904 | 8461,3,3169 | 8462,5,3094 | 8464,5,2495 |
| 8466,1 | 8467,5,1729 | 8468,4,431 | 8469,5,103 | 8472,3,3466 | 8474,7,4058 | 8475,2,1105 | 8477,3,1079 | 8480,2,677 | 8483,2,2519 |
| 8485,3,3309 | 8486,5,150 | 8488,5,2213 | 8490,3,1483 | 8491,8,2764 | 8493,6,2120 | 8494,4,2061 | 8496,2,1861 | 8498,3,3453 | 8499,8,1047 |
| 8501,3,1745 | 8504,3,815 | 8507,2,353 | 8509,12,3516 | 8512,3,3298 | 8514,3,1597 | 8515,5,3443 | 8517,8,3846 | 8520,2,985 | 8523,2,316 |
| 8525,3,2309 | 8528,2,221 | 8531,2,326 | 8533,5,3065 | 8534,2,1685 | 8536,3,100 | 8538,1 | 8539,15,2703 | 8541,3,3989 | 8542,4,4229 |
| 8544,2,2101 | 8546,3,2645 | 8547,8,981 | 8549,9,529 | 8552,2,3365 | 8554,3,2227 | 8555,9,2313 | 8557,3,2557 | 8560,3,724 | 8561,2,2045 |
| 8562,1 | 8563,3,3403 | 8565,5,1627 | 8567,6,2519 | 8568,3,1331 | 8570,6,2883 | 8571,2,1003 | 8572,1 | 8573,3,75 | 8574,5,4095 |
| 8576,3,2078 | 8578,3,1215 | 8579,2,1403 | 8581,12,3493 | 8584,3,1005 | 8587,5,95 | 8589,3,37 | 8590,7,974 | 8592,3,1024 | 8594,3,2511 |
| 8595,2,2239 | 8596,1 | 8597,8,2898 | 8598,2,7 | 8600,2,1517 | 8603,2,767 | 8605,6,3378 | 8606,5,1576 | 8608,3,892 | 8610,3,590 |
| 8611,3,775 | 8613,6,2636 | 8616,19,1483 | 8619,2,1639 | 8621,5,839 | 8622,5,3527 | 8624,3,1604 | 8626,1 | 8627,2,182 | 8628,2,283 |
| 8629,6,3886 | 8630,5,3871 | 8632,3,243 | 8634,3,3775 | 8635,5,2021 | 8637,3,2141 | 8640,5,1347 | 8642,5,836 | 8643,2,991 | 8645,6,1916 |
| 8648,2,2477 | 8651,2,1652 | 8653,7,991 | 8656,19,433 | 8659,3,3739 | 8661,14,3263 | 8662,7,1095 | 8664,13,560 | 8667,2,223 | 8668,1 |
| 8669,3,1425 | 8672,2,2741 | 8675,2,4295 | 8676,1 | 8677,6,748 | 8678,11,1963 | 8680,3,2095 | 8683,5,3833 | 8685,5,1171 | 8687,3,1121 |
| 8688,2,2593 | 8690,5,236 | 8691,2,1540 | 8692,1 | 8693,14,1479 | 8696,3,410 | 8698,1 | 8699,3,479 | 8701,3,3837 | 8702,17,775 |
| 8704,3,352 | 8706,3,3314 | 8707,5,329 | 8709,3,3695 | 8710,5,134 | 8712,2,685 | 8715,2,1615 | 8716,8,265 | 8717,9,2293 | 8720,3,243 |
| 8723,9,3121 | 8725,7,1703 | 8726,5,163 | 8728,3,3114 | 8730,1 | 8731,10,1988 | 8733,5,1795 | 8736,2,3253 | 8738,4,3391 | 8739,2,202 |
| 8740,1 | 8741,3,2259 | 8744,3,272 | 8746,1 | 8747,2,176 | 8749,6,643 | 8752,3,1089 | 8755,11,1633 | 8757,6,26 | 8758,8,3851 |
| 8760,3,247 | 8761,7,4175 | 8763,2,223 | 8764,10,2511 | 8765,5,3477 | 8768,8,261 | 8771,2,1694 | 8773,3,1 | 8774,2,233 | 8776,3,1375 |
| 8778,3,932 | 8779,3,4339 | 8781,3,2053 | 8782,5,3950 | 8784,5,1107 | 8786,3,327 | 8787,2,2131 | 8788,4,3413 | 8789,8,1396 | 8790,2,1405 |
| 8792,3,932 | 8794,3,382 | 8795,16,1319 | 8797,3,1123 | 8800,3,495 | 8802,1 | 8803,5,211 | 8805,3,2351 | 8808,3,3697 | 8810,4,3847 |
| 8811,2,1084 | 8813,3,1661 | 8816,3,3987 | 8818,1 | 8819,2,155 | 8820,1 | 8821,13,1933 | 8822,2,2321 | 8824,7,3334 | 8827,3,1443 |
| 8829,5,4229 | 8832,5,396 | 8835,2,2182 | 8836,1 | 8837,8,3411 | 8840,3,731 | 8843,9,3151 | 8845,6,2280 | 8846,10,1645 | 8848,3,1275 |
| 8851,3,2587 | 8853,10,951 | 8854,7,1160 | 8856,3,3646 | 8858,4,31 | 8859,2,3454 | 8860,1 | 8861,7,3049 | 8864,2,2081 | 8866,1 |
| 8867,2,653 | 8869,8,3100 | 8872,3,4146 | 8875,5,2453 | 8877,3,1111 | 8880,6,3363 | 8882,14,2165 | 8883,2,2812 | 8885,3,4215 | 8888,2,4421 |
| 8891,2,101 | 8893,3,4281 | 8894,5,3570 | 8896,3,2901 | 8899,5,1249 | 8901,6,1784 | 8902,5,89 | 8904,5,2813 | 8906,3,627 | 8907,2,2359 |
| 8909,3,1991 | 8912,3,2819 | 8914,3,2298 | 8915,2,3695 | 8917,3,1497 | 8918,2,137 | 8920,3,2923 | 8922,1 | 8923,8,616 | 8925,3,653 |
| 8928,2,3937 | 8931,2,1498 | 8932,1 | 8933,5,695 | 8936,11,4011 | 8939,2,644 | 8941,3,3403 | 8942,2,191 | 8944,3,1039 | 8947,10,1510 |
| 8949,5,4231 | 8950,16,411 | 8952,2,4453 | 8954,9,804 | 8955,2,331 | 8957,7,97 | 8960,2,3269 | 8962,1 | 8963,2,23 | 8965,6,2017 |
| 8968,3,586 | 8970,1 | 8971,12,1350 | 8973,5,1447 | 8976,3,2615 | 8978,5,2120 | 8979,2,988 | 8981,9,1863 | 8984,3,1458 | 8987,3,4119 |
| 8989,5,4241 | 8992,12,1161 | 8995,5,833 | 8996,2,3023 | 8997,6,163 | 8998,9,815 | 9000,2,337 | 9003,2,1852 | 9005,5,3969 | 9008,2,1157 |
| 9010,1 | 9011,2,1262 | 9013,5,3833 | 9015,5,4219 | 9016,3,3487 | 9019,3,2727 | 9021,16,1147 | 9024,2,817 | 9027,2,2194 | 9028,1 |
| 9029,3,2211 | 9030,3,3011 | 9032,3,4232 | 9035,2,776 | 9037,3,4377 | 9038,2,839 | 9040,3,3063 | 9043,11,1549 | 9045,5,571 | 9046,7,3402 |
| 9048,9,101 | 9051,2,4177 | 9053,9,3495 | 9056,2,2105 | 9058,1 | 9059,2,206 | 9061,6,3907 | 9064,3,2757 | 9066,3,3646 | 9067,3,1999 |
| 9069,6,4253 | 9070,5,3763 | 9072,3,3761 | 9073,4,504 | 9075,2,2131 | 9077,3,1767 | 9080,2,833 | 9082,3,606 | 9083,2,806 | 9085,3,1725 |
| 9087,7,2161 | 9088,3,2626 | 9090,4,2311 | 9091,5,1859 | 9093,8,3156 | 9096,2,913 | 9098,3,915 | 9099,2,130 | 9101,3,3533 | 9102,2,1591 |
| 9104,2,881 | 9107,2,1775 | 9109,3,2745 | 9110,14,3999 | 9112,3,838 | 9115,7,1217 | 9117,5,1207 | 9118,7,1799 | 9120,2,4153 | 9122,3,1763 |
| 9123,2,2167 | 9124,4,4191 | 9125,6,600 | 9128,3,1905 | 9131,2,2768 | 9133,5,1421 | 9136,3,1090 | 9139,7,2251 | 9141,5,2239 | 9144,2,2005 |
| 9146,9,1902 | 9147,2,2341 | 9149,3,477 | 9152,3,2132 | 9155,2,797 | 9157,3,2869 | 9160,5,28 | 9163,3,2955 | 9165,11,2871 | 9166,5,4090 |
| 9167,4,3208 | 9168,6,339 | 9171,2,2167 | 9172,1 | 9173,3,767 | 9174,2,3823 | 9176,2,3773 | 9178,3,1440 | 9179,3,1607 | 9180,1 |
| 9181,5,37 | 9183,3,937 | 9184,3,1780 | 9187,7,2405 | 9189,22,3012 | 9192,2,2821 | 9194,3,1437 | 9195,2,1573 | 9196,7,4541 | 9197,3,2519 |
| 9200,2,3425 | 9202,1 | 9203,7,3841 | 9205,7,2539 | 9208,8,1187 | 9211,5,2837 | 9213,3,1931 | 9216,7,3337 | 9219,2,259 | 9220,1 |
| 9221,3,81 | 9222,2,3433 | 9224,2,4241 | 9226,1 | 9227,2,53 | 9229,10,2867 | 9230,2,623 | 9232,3,1347 | 9235,7,2839 | 9236,2,2351 |
| 9237,8,297 | 9240,3,1717 | 9243,2,349 | 9245,7,1691 | 9246,2,1429 | 9248,3,2826 | 9251,2,1925 | 9253,3,3811 | 9254,2,2549 | 9256,3,3172 |
| 9259,5,829 | 9261,3,863 | 9264,7,499 | 9266,3,3482 | 9267,2,1831 | 9269,3,4367 | 9272,2,1457 | 9275,2,257 | 9277,3,417 | 9280,3,3160 |
| 9282,1 | 9283,10,4568 | 9285,5,2681 | 9286,11,4241 | 9288,3,367 | 9291,2,652 | 9292,1 | 9293,5,553 | 9296,3,2277 | 9299,2,110 |
| 9301,6,2355 | 9304,3,670 | 9307,7,3303 | 9309,5,249 | 9312,2,2269 | 9314,8,2149 | 9315,5,2189 | 9317,5,4379 | 9318,7,4171 | 9320,3,2354 |
| 9322,1 | 9323,2,188 | 9325,3,657 | 9326,2,695 | 9328,5,4628 | 9331,16,1621 | 9333,6,1745 | 9336,3,1900 | 9338,3,716 | 9339,8,2504 |
| 9340,1 | 9341,3,1199 | 9342,2,2749 | 9344,3,1368 | 9346,3,2875 | 9347,2,2300 | 9348,1 | 9349,5,4529 | 9352,3,1458 | 9354,13,2195 |
| 9355,3,739 | 9357,3,283 | 9360,3,4192 | 9362,3,2424 | 9363,2,451 | 9365,3,1889 | 9368,5,1186 | 9370,1 | 9371,2,521 | 9373,3,4153 |
| 9374,2,3041 | 9376,3,4230 | 9379,8,373 | 9381,3,593 | 9384,2,3085 | 9387,5,1377 | 9388,9,4638 | 9389,5,4693 | 9392,2,569 | 9395,2,425 |
| 9396,1 | 9397,11,2407 | 9400,3,2488 | 9403,5,1727 | 9405,6,419 | 9406,9,2792 | 9408,3,2192 | 9410,9,1785 | 9411,2,1225 | 9412,4,4439 |
| 9413,3,395 | 9416,3,4010 | 9418,1 | 9419,2,1169 | 9420,1 | 9421,3,493 | 9422,2,2345 | 9424,3,967 | 9426,9,2033 | 9427,12,1525 |
| 9428,5,1742 | 9429,10,2766 | 9430,9,3153 | 9432,7,4608 | 9434,3,2427 | 9435,2,226 | 9436,1 | 9437,5,863 | 9438,2,4333 | 9440,5,4489 |
| 9443,2,1418 | 9445,3,375 | 9446,2,665 | 9448,3,40 | 9451,5,4049 | 9452,8,1127 | 9453,15,1633 | 9456,2,3733 | 9458,3,2147 | 9459,2,3070 |
| 9460,10,895 | 9461,6,482 | 9462,2,85 | 9464,3,2907 | 9466,1 | 9467,2,1370 | 9469,3,1965 | 9472,3,622 | 9474,3,3427 | 9475,16,453 |
| 9477,7,1383 | 9480,2,3313 | 9482,5,2603 | 9483,2,1783 | 9485,3,3669 | 9488,2,1697 | 9490,1 | 9491,3,4427 | 9493,8,3886 | 9495,3,4421 |
| 9496,5,149 | 9498,3,1291 | 9499,12,3721 | 9501,3,3469 | 9504,2,4009 | 9505,4,1743 | 9506,5,2573 | 9507,2,3961 | 9509,5,1655 | 9512,3,741 |
| 9514,3,1791 | 9515,2,3644 | 9517,10,2116 | 9520,3,43 | 9523,8,4531 | 9525,3,2245 | 9526,5,1997 | 9528,3,992 | 9531,2,4732 | 9532,1 |
| 9533,6,752 | 9536,3,428 | 9538,1 | 9539,2,80 | 9541,10,155 | 9544,3,303 | 9546,1 | 9547,3,2187 | 9549,3,2399 | 9550,5,419 |
| 9552,7,2306 | 9554,3,2001 | 9555,2,2200 | 9556,9,4729 | 9557,3,2909 | 9560,3,353 | 9563,2,938 | 9565,5,317 | 9568,3,1098 | 9571,5,1307 |
| 9572,2,4619 | 9573,16,700 | 9574,10,313 | 9576,5,1433 | 9579,2,4696 | 9581,5,3625 | 9584,3,993 | 9586,1 | 9587,2,1937 | 9589,3,1413 |
| 9592,3,39 | 9595,3,1711 | 9596,5,755 | 9597,3,1807 | 9600,3,317 | 9602,3,2252 | 9603,2,2113 | 9604,4,4007 | 9605,3,41 | 9606,3,3203 |
| 9608,2,2213 | 9611,2,1397 | 9612,1 | 9613,3,99 | 9616,3,52 | 9618,1 | 9619,7,221 | 9621,5,1001 | 9624,3,2957 | 9626,3,300 |
| 9627,2,742 | 9628,1 | 9629,5,1679 | 9632,3,4524 | 9635,3,2403 | 9637,10,614 | 9638,2,713 | 9640,7,1906 | 9642,1 | 9643,5,611 |
| 9645,3,1861 | 9646,7,3296 | 9648,3,886 | 9650,5,587 | 9651,2,1993 | 9653,3,3263 | 9656,3,2865 | 9659,2,653 | 9660,1 | 9661,3,4303 |
| 9662,2,1859 | 9664,6,879 | 9667,7,4005 | 9669,3,1429 | 9670,8,4325 | 9672,3,397 | 9675,2,382 | 9676,1 | 9677,5,3239 | 9680,3,1784 |
| 9683,2,3656 | 9685,5,3073 | 9688,3,4111 | 9691,3,4279 | 9693,5,1891 | 9694,4,81 | 9696,3,4528 | 9698,3,1901 | 9699,2,547 | 9701,3,2099 |
| 9703,3,3673 | 9704,3,1611 | 9706,7,1432 | 9707,2,965 | 9709,6,1963 | 9710,2,3917 | 9712,3,2011 | 9715,3,1735 | 9717,3,859 | 9718,5,617 |
| 9720,5,3456 | 9722,3,1802 | 9723,2,568 | 9724,10,4333 | 9725,3,1019 | 9726,5,398 | 9728,2,89 | 9731,2,1853 | 9732,1 | 9733,11,3925 |
| 9736,3,2985 | 9739,5,4015 | 9741,5,2635 | 9742,5,3499 | 9744,2,3133 | 9747,2,1204 | 9748,1 | 9749,8,3582 | 9752,3,3351 | 9755,2,50 |
| 9757,7,631 | 9760,3,2713 | 9763,5,4645 | 9764,2,1547 | 9765,6,4142 | 9768,2,133 | 9771,2,1912 | 9773,3,3113 | 9776,2,3485 | 9778,3,2887 |
| 9779,2,4190 | 9781,6,739 | 9784,3,1515 | 9787,10,2877 | 9789,3,1619 | 9792,3,1819 | 9794,3,348 | 9795,2,1555 | 9797,5,109 | 9800,3,1164 |
| 9802,1 | 9803,2,497 | 9805,3,747 | 9806,2,287 | 9808,3,2686 | 9809,2,80 | 9811,5,3929 | 9812,4,3683 | 9813,9,4901 | 9815,4,4387 |
| 9816,3,1100 | 9818,4,211 | 9819,5,1769 | 9821,3,3599 | 9824,2,209 | 9826,3,2166 | 9827,2,1754 | 9829,3,1041 | 9832,5,2794 | 9834,3,3265 |
| 9835,19,4111 | 9836,11,3083 | 9837,3,1733 | 9838,4,1133 | 9840,2,4213 | 9842,3,1233 | 9843,2,1714 | 9845,8,1563 | 9848,3,3422 | 9850,1 |
| 9851,9,4789 | 9853,6,186 | 9856,5,959 | 9858,1 | 9859,8,1732 | 9861,3,3545 | 9862,7,335 | 9864,2,4633 | 9866,3,1437 | 9867,2,463 |
| 9869,5,193 | 9872,2,3377 | 9875,2,3578 | 9877,3,3397 | 9880,3,1215 | 9881,8,1055 | 9882,1 | 9883,11,1609 | 9885,3,901 | 9888,2,241 |
| 9891,2,565 | 9892,9,4011 | 9893,3,603 | 9894,3,3299 | 9896,3,4280 | 9898,3,3186 | 9899,2,3218 | 9900,1 | 9901,3,639 | 9902,4,3413 |
| 9904,7,1153 | 9906,1 | 9907,5,445 | 9909,9,2635 | 9910,5,4714 | 9912,2,4477 | 9915,2,3568 | 9917,3,3561 | 9920,2,2945 | 9922,1 |
| 9923,2,3503 | 9924,2,1387 | 9925,3,993 | 9928,3,288 | 9931,12,640 | 9933,5,4579 | 9934,4,1697 | 9936,3,2335 | 9938,8,4771 | 9939,2,2167 |
| 9940,1 | 9941,3,1077 | 9944,11,972 | 9947,2,2798 | 9948,1 | 9949,3,1957 | 9952,3,3204 | 9955,3,2127 | 9957,12,194 | 9958,7,408 |
| 9960,2,1441 | 9962,3,551 | 9963,2,4126 | 9965,5,167 | 9968,3,1836 | 9971,2,3092 | 9973,6,786 | 9976,3,3351 | 9979,8,2572 | 9981,3,4871 |
| 9984,3,1439 | 9987,2,1027 | 9989,18,616 | 9992,2,3209 | 9994,3,2026 | 9995,2,701 | 9997,3,2679 | 10000,7,1629 | | |

## 7. Tests

Some computations have been done on a PC with a Pentium IV processor at 2.6 Ghz running Linux. The test program was written in `C++` using `NTL 5.3.1` [NTL] and compares the efficiency of irreducible pentanomials against redundant trinomials for some basic operations within extension fields of $\mathbb{F}_2$ of prime degree between 50 and 400. For both systems of representation, namely $\mathbb{F}_2[x]/\big(p(x)\big)$ and $\mathbb{F}_2[x]/\big(t(x)\big)$, we give in Table 1 the running times and the respective speed up (in percent) for

- the reduction of a polynomial of degree $2n-2$ (resp. $2m-2$) modulo $p(x)$ (resp. $t(x)$).
- the squaring of an element of $\mathbb{F}_{2^n}$
- the multiplication of two elements of $\mathbb{F}_{2^n}$
- the exponentiation of an element of $\mathbb{F}_{2^n}$ to an exponent less than $2^n$.

The unit used is $10^{-7}$s for reduction, squaring and multiplication. It is $10^{-5}$s for exponentiation.
Redundant trinomials are not well suited for inversions, at least when computed with an extended gcd computations. Results show that inversions are about 15% slower with redundant trinomials.
Prime extension degrees 59, 197, 211, 277, 311, 317, 331, 347, 389, and 397 are quite particular. Indeed for these $n$ there exists a trinomial of degree $m = \lceil n/32 \rceil \times 32$ with an irreducible factor of degree $n$. Such a polynomial is called an *optimal redundant trinomial*. For all these degrees, except for $n = 317$, another redundant trinomial of smaller degree exists. However tests show that the results are much better with optimal trinomials. Thus when it is possible, these polynomials are used instead. With the same conventions as previously they are

| | | | | |
|---|---|---|---|---|
| $59, 5, 9$ | $197, 27, 103$ | $211, 13, 67$ | $277, 11, 83$ | $293, 27, 91$ |
| $311, 9, 33$ | $331, 21, 81$ | $347, 5, 127$ | $389, 27, 205$ | $397, 19, 175$ |

Unfortunately the extension degrees which allow the use of optimal redundant trinomials are quite rare. However an *optimal redundant quadrinomial* whose degree is a multiple of 32 and having an irreducible factor of degree $n$ are much easier to find for a given $n$. Tests with `NTL` showed that in some cases optimal redundant quadrinomials give better result than nonoptimal redundant trinomials and even than irreducible trinomials.
In Table 2 we perform the same computation for bigger degrees. The units are in $\mu$s for reduction and squaring, $10^{-5}$s for multiplication and $10^{-4}$s for exponentiation.
Finally, we have done some computations on elliptic curves defined over finite fields represented with pentanomials and redundant trinomials. Table 3 contains the running times of an addition and a doubling in $\mu$s with Montgomery's method. The times for scalar multiplications, also with Montgomery's method, are in ms.

| | | Red. | | | Sqr. | | | Mul. | | | Exp. | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $n$ | $\deg \delta$ | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* |
| 53 | 8 | 1.63 | 1.37 | 15.95 | 2.17 | 1.77 | 18.43 | 3.51 | 3.04 | 13.39 | 1.82 | 1.53 | 15.93 |
| 59 | 5 | 1.64 | 0.89 | 45.73 | 2.17 | 1.37 | 36.87 | 3.51 | 2.63 | 25.07 | 2.01 | 1.39 | 30.85 |
| 61 | 5 | 1.63 | 1.33 | 18.40 | 2.20 | 1.70 | 22.73 | 3.49 | 4.87 | −39.54 | 2.07 | 2.05 | 0.97 |
| 67 | 9 | 1.57 | 1.31 | 16.56 | 2.18 | 1.80 | 17.43 | 5.37 | 4.99 | 7.08 | 2.67 | 2.28 | 14.61 |
| 83 | 2 | 2.01 | 1.48 | 26.37 | 2.46 | 1.89 | 23.17 | 5.70 | 5.40 | 5.26 | 3.51 | 3.00 | 14.53 |
| 101 | 2 | 1.88 | 1.50 | 20.21 | 2.42 | 2.01 | 16.94 | 6.60 | 6.08 | 7.88 | 4.44 | 3.88 | 12.61 |
| 107 | 2 | 1.91 | 1.50 | 21.47 | 2.49 | 2.02 | 18.88 | 6.53 | 6.02 | 7.81 | 4.64 | 4.05 | 12.72 |
| 109 | 9 | 1.93 | 1.64 | 15.03 | 2.47 | 2.16 | 12.55 | 6.53 | 6.26 | 4.13 | 4.76 | 4.33 | 9.03 |
| 131 | 7 | 2.04 | 1.50 | 26.47 | 2.62 | 2.14 | 18.32 | 10.28 | 10.07 | 2.04 | 7.26 | 6.28 | 13.50 |
| 139 | 3 | 2.37 | 1.87 | 21.10 | 3.00 | 2.16 | 28.00 | 10.77 | 10.24 | 4.92 | 8.19 | 6.95 | 15.14 |
| 149 | 2 | 2.69 | 1.86 | 30.86 | 3.24 | 2.39 | 26.23 | 11.02 | 10.55 | 4.26 | 9.15 | 7.68 | 16.07 |
| 157 | 7 | 2.73 | 1.82 | 33.33 | 3.31 | 2.39 | 27.79 | 11.01 | 12.46 | −13.17 | 9.73 | 8.92 | 8.32 |
| 163 | 8 | 2.50 | 1.72 | 31.20 | 3.02 | 2.28 | 24.50 | 13.31 | 12.08 | 9.24 | 10.65 | 8.90 | 16.43 |
| 173 | 3 | 2.73 | 1.90 | 30.40 | 3.38 | 2.47 | 26.92 | 13.00 | 12.39 | 4.69 | 11.61 | 9.87 | 14.99 |
| 179 | 2 | 3.01 | 2.15 | 28.57 | 3.61 | 2.67 | 26.04 | 13.09 | 12.66 | 3.28 | 12.90 | 10.66 | 17.36 |
| 197 | 27 | 3.03 | 1.51 | 50.17 | 3.78 | 2.14 | 43.39 | 15.16 | 13.50 | 10.95 | 14.50 | 10.74 | 25.93 |
| 211 | 13 | 3.43 | 1.55 | 54.81 | 4.14 | 2.14 | 48.31 | 15.35 | 13.50 | 12.05 | 16.49 | 11.50 | 30.26 |
| 227 | 2 | 3.17 | 2.27 | 28.39 | 4.01 | 2.98 | 25.69 | 17.08 | 15.51 | 9.19 | 18.29 | 15.53 | 15.09 |
| 229 | 3 | 3.25 | 2.35 | 27.69 | 4.18 | 3.03 | 27.51 | 16.70 | 15.28 | 8.50 | 18.24 | 15.75 | 13.65 |
| 251 | 2 | 3.70 | 2.52 | 31.89 | 4.72 | 3.07 | 34.96 | 16.79 | 15.27 | 9.05 | 21.14 | 17.70 | 16.27 |
| 269 | 5 | 3.71 | 3.04 | 18.06 | 4.62 | 3.77 | 18.40 | 27.05 | 26.49 | 2.07 | 28.65 | 26.51 | 7.47 |
| 277 | 11 | 4.12 | 1.97 | 52.18 | 4.80 | 2.70 | 43.75 | 27.43 | 25.37 | 7.51 | 30.44 | 23.42 | 23.06 |
| 283 | 3 | 4.08 | 3.16 | 22.55 | 4.86 | 3.89 | 19.96 | 27.43 | 26.47 | 3.50 | 31.22 | 28.30 | 9.35 |
| 293 | 27 | 3.81 | 2.12 | 44.36 | 4.69 | 2.88 | 38.59 | 31.09 | 29.12 | 6.34 | 34.15 | 28.03 | 17.92 |
| 307 | 5 | 4.50 | 2.96 | 34.22 | 5.32 | 3.67 | 31.02 | 31.70 | 30.11 | 5.02 | 38.10 | 32.48 | 14.75 |
| 311 | 9 | 4.52 | 2.09 | 53.76 | 5.33 | 2.90 | 45.59 | 31.74 | 29.11 | 8.29 | 38.58 | 29.63 | 23.20 |
| 317 | 3 | 4.52 | 2.12 | 53.10 | 5.36 | 2.87 | 46.46 | 31.74 | 29.12 | 8.25 | 39.18 | 30.01 | 23.40 |
| 331 | 21 | 4.57 | 2.26 | 50.55 | 5.58 | 3.18 | 43.01 | 35.95 | 33.54 | 6.70 | 44.07 | 35.56 | 19.31 |
| 347 | 5 | 4.98 | 2.20 | 55.82 | 5.83 | 3.12 | 46.48 | 36.18 | 33.53 | 7.32 | 47.41 | 37.04 | 21.87 |
| 349 | 6 | 4.99 | 3.16 | 36.67 | 5.83 | 4.06 | 30.36 | 36.17 | 37.58 | −3.90 | 47.77 | 43.24 | 9.48 |
| 373 | 3 | 5.18 | 3.51 | 32.24 | 6.23 | 4.33 | 30.50 | 38.44 | 36.55 | 4.92 | 53.66 | 45.72 | 14.80 |
| 379 | 3 | 5.20 | 3.34 | 35.77 | 6.25 | 4.26 | 31.84 | 38.44 | 36.67 | 4.60 | 54.44 | 46.21 | 15.12 |
| 389 | 5 | 4.50 | 3.29 | 26.89 | 5.50 | 4.15 | 24.55 | 41.67 | 40.44 | 2.95 | 56.47 | 50.41 | 10.73 |
| 389 | 27 | 4.56 | 2.41 | 47.15 | 5.52 | 3.35 | 39.31 | 41.67 | 39.40 | 5.45 | 56.13 | 46.48 | 17.19 |
| 397 | 19 | 5.24 | 2.39 | 54.39 | 6.20 | 3.36 | 45.81 | 42.14 | 39.41 | 6.48 | 60.50 | 47.41 | 21.64 |

TABLE 1

## 8. CONCLUSION

The improvement is about 20% for reductions and squarings. For multiplications it is usually less than 5%. Testing the equality of two elements is a costly operation, and should be avoided if possible.

This work naturally extends to other fields, in particular extension fields of characteristic 3. It can be applied to larger characteristic as well. Indeed Mersenne prime numbers or primes of the form $2^n \pm c$ with $c$ small are used to define prime

| | | Red. | | | Sqr. | | | Mul. | | | Exp. | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $n$ | $\deg \delta$ | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* |
| 1019 | 2 | 1.22 | 0.75 | 38.52 | 1.41 | 0.96 | 31.91 | 1.36 | 1.32 | 2.94 | 39.84 | 33.97 | 14.73 |
| 2499 | 2 | 2.57 | 1.80 | 29.96 | 2.94 | 2.05 | 30.27 | 7.60 | 7.50 | 1.32 | 365.91 | 340.75 | 6.88 |
| 5013 | 9 | 4.68 | 3.31 | 29.27 | 5.45 | 4.00 | 26.61 | 22.68 | 22.54 | 0.62 | 1840.55 | 1757.94 | 4.49 |
| 7597 | 17 | 7.87 | 5.05 | 35.83 | 8.65 | 5.97 | 30.98 | 35.34 | 35.09 | 0.71 | 4133.90 | 3896.40 | 5.75 |
| 9995 | 2 | 9.92 | 6.59 | 33.57 | 11.22 | 7.78 | 30.66 | 67.96 | 67.62 | 0.50 | 9561.80 | 9180.50 | 3.99 |

TABLE 2

| | | Dbl. | | | Add. | | | Mul. | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $n$ | $\deg \delta$ | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* | *pent.* | *tri.* | *gain* |
| 163 | 8 | 1.35 | 1.24 | 8.15 | 3.60 | 3.33 | 7.50 | 1.79 | 1.61 | 10.06 |
| 197 | 27 | 1.52 | 1.09 | 28.29 | 4.07 | 3.49 | 14.25 | 2.42 | 2.10 | 13.22 |
| 277 | 6 | 1.81 | 1.57 | 13.26 | 6.72 | 6.45 | 4.02 | 5.69 | 5.41 | 4.92 |
| 317 | 3 | 1.91 | 1.30 | 31.94 | 7.61 | 6.74 | 11.43 | 7.41 | 6.65 | 10.26 |

TABLE 3

fields of large characteristic and Optimal Extension Fields [BP 2001] because of the fast integer reduction they provide. However these primes are quite rare, but when $N = 2^n \pm c$ is not prime but has a large prime factor $p$ the same kind of idea apply, namely working in $\mathbb{F}_p$ by actually computing in $\mathbb{Z}/N\mathbb{Z}$.

## ACKNOWLEDGMENT

The author would like to praise the kind reaction of Richard Brent and Paul Zimmermann who pointed out their preprints and the articles of Blake *et al.* and Tromp *et al.*

## REFERENCES

[BB$^+$ 1989] F. BERGERON, J. BERSTEL, S. BRLEK & C. DUBOC, *Addition chains using continued fractions*, J. Algorithms **10** N°3 (1989), 403–412.

[BBB 1994] F. BERGERON, J. BERSTEL & S. BRLEK, *Efficient computation of addition chains*, Journ. de Théorie des Nombres de Bordeaux **6** (1994), 21–38.

[BC 1990] J. BOS & M. COSTER, *Addition chain heuristics*, Advances in Cryptology–Proceedings of crypto'89, Lecture Notes in Comput. Sci., vol. 435, Springer-Verlag, Berlin, 1990, pp. 400–407.

[BGL 1994] I. F. BLAKE, S. GAO & R. J. LAMBERT, *Constructive problems for irreducible polynomials over finite fields*, Information Theory and Applications, vol. 793, Springer-Verlag, Berlin, 1994, pp. 1–23.

[BGL 1996] ———, *Construction and distribution problems for irreducible trinomials over finite fields*, 1996, pp. 19–32.
See `http://www.math.clemson.edu/~sgao/pub.html`

[BP 2001] D. V. BAILEY & C. PAAR, *Efficient arithmetic in finite field extensions with application in elliptic curve cryptography*, Journal of Cryptology **14** N°3 (2001), 153–176.
See `http://citeseer.nj.nec.com/bailey00efficient.html`

[BZ] R. Brent & P. Zimmermann, *Algorithms for finding almost irreducible and almost primitive trinomials.* Primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams, The Fields Institute, Toronto, to be published by the American Mathematical Society.
See `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pd/rpb212.pdf`

[BZ 2003] ———, *Random number generators with period divisible by a mersenne prime*, Computational Science and its Applications - ICCSA 2003, vol. 2667, Springer-Verlag, Berlin, 2003, pp. 1–10.
See `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pd/rpb211.pdf`

[Doche] C. Doche, *A table of redundant trinomials in characteristic* 2 *up to the degree* 10000.
See `http://www.math.u-bordeaux.fr/~cdoche/documents/redundant.gp.gz`

[Fre 2001] G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, Fifth International Conference on Finite Fields and Applications (D. Jungnickel & H. Niederreiter, eds.), Springer-Verlag, Berlin, 2001, pp. 128–161.

[GG 1996] J. von zur Gathen & J. Gerhard, *Arithmetic and factorization of polynomials over* $\mathbb{F}_2$, 1996.
See `http://math-www.uni-paderborn.de/~aggathen/Publications/polyfactTR.ps`

[GHS 2002] P. Gaudry, F. Hess & N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, Journal of Cryptology **15** N°1 (2002), 19–46, Online publication: 29 August 2001.
See `http://www.hpl.hp.com/techreports/2000/HPL-2000-10.html`

[GN] J. von zur Gathen & M. Nöcker, *Polynomial and normal bases for finite fields.* To appear.
See `http://www-math.upb.de/~aggathen/Publications/gatnoe03b.pdf`

[IT 1988] T. Itoh & S. Tsujii, *A fast algorithm for computing multiplicative inverses in* $GF(2^m)$ *using normal bases*, Information and Computation **78** N°3 (1988), 171–177.

[Jeb 1993] T. Jebelean, *An algorithm for exact division*, J. Symbolic Computation **15** N°2 (1993), 169–180.

[MQ 2001] A. Menezes & M. Qu, *Analysis of the Weil descent attack of Gaudry, Hess and Smart*, Topics in Cryptology – CT-RSA 2001, Lecture Notes in Comput. Sci., vol. 2020, Springer-Verlag, Berlin, 2001, pp. 308–318.
See `http://citeseer.nj.nec.com/396217.html`

[NTL] V. Shoup, *NTL: A Library for doing Number Theory, ver. 5.3.1.*
See `http://www.shoup.net/`

[Nöc 1996] M. Nöcker, *Exponentiation in finite fields: theory and practice*, Diplomarbeit im fach informatik, Universität Paderborn, 1996.

[Ser 1998] G. Seroussi, *Table of low–weight binary irreducible polynomials*, Tech. Report HPL–98–135, Hewlett–Packard, August 1998.
See `http://www.hpl.hp.com/techreports/98/HPL-98-135.pdf`

[SOO 1995] R. Schroeppel, H. Orman & S. O'Malley, *Fast key exchange with elliptic curve systems*, Tech. report, Department of Computer Science. The University of Arizona, 1995.

[TZZ 1997] J. Tromp, L. Zhang & Y. Zhao, *Small weight bases for Hamming codes*, Theoretical Computer Science **181** N°2 (1997), 337–345.

[WH+] H. Wu, M. A. Hasan, I. F. Blake & S. Gao, *Finite field multiplier using redundant representation.*
See `citeseer.nj.nec.com/wu01finite.html`

Division of ICS, Building E6A, Macquarie University, NSW 2109 Australia.
*E-mail address*: doche@ics.mq.edu.au