Modulo primality test.

1. Abstract.

Verifying large prime numbers is a time-consuming proces, even with modern day computers.
This article describes the "modulo primality test" that combines the segmented prime spiral, modular arithmetic and the primorial sieve. The "modulo primality test" can be used to factorize RSA-numbers.
In the segmented prime spiral with **one** segment each integer is identified as an unique member of the Eastward family of quadratic polynomials with only two terms. By way of modular arithmetic the number of digits is reduced when checking a large integer for a possible divisor. In addition the primorial sieve can be used to deselect sets of divisors.
The modulo primality test can also be used as another methode to check the correctness of computercalculations.

2. The prime spiral with one segment.

The modulo primality test is based on the prime spiral with **one** segment. This prime spiral is derived from the Ulam spiral with startvalue 0 when placed in a Cartesian coordinate system (appendix A).
There is an infinite set of families of segmented prime spirals. The Ulam spiral has four segments.

The segmented prime spirals are unusual since integers on the seam appear twice. These doubled integers disappear behind the overlap when putting a prime spiral together, like when folding the prime spiral with one segment into a cone (Fig. 1), or the SE main diagnonal in the Ulam spiral (appendix A).

Each integer in the prime spiral with **one** segment is member of the Eastward family of functions
$f_{1,c}(n_E) = 1n^2 + 0n + c = n^2 + c$ with $-n < c \leq n$ which has just two terms (Fig. 1).
For instance the integer $g = 90$ with $n = \lfloor \sqrt{g} \rceil$ has the parameters $n = 9$ and $c = 9$ and is thus found on the NE main diagonal at the location $(x, y) = (n, c) = (9, 9)$. The location $(10, -10)$ of $g = 90$ on the SE main diagonal does not comply with the definition of the families of functions (appendix A).
Note that the integer $g = 90$ also belongs to $f_{1,0}(n_{NE}) = 1n^2 + 1n + 0$ and $f_{1,18}(n_{SE}) = 1n^2 - 1n + 18$ with $n = \lfloor \sqrt{g} \rceil$

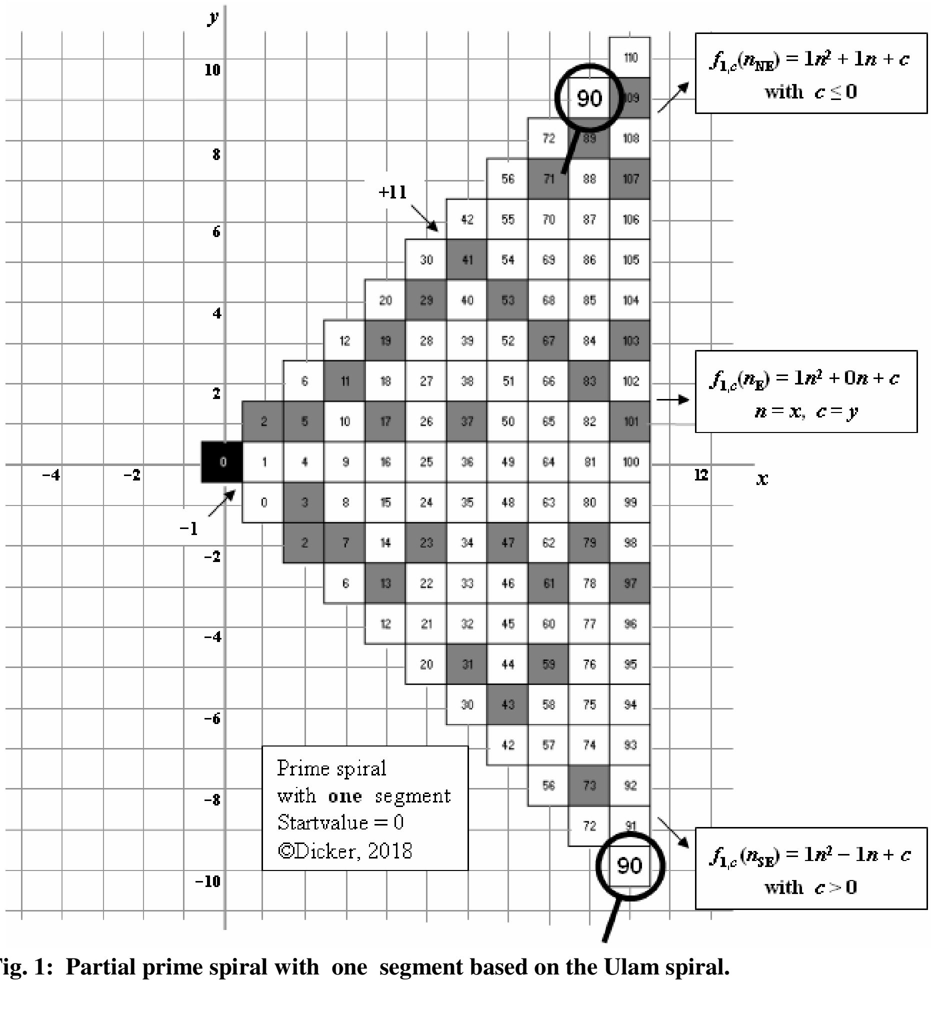

Fig. 1: Partial prime spiral with one segment based on the Ulam spiral.

3. The modulo primality test.

The simplest primality test to verify if an integer g is a prime number is trial division.
Find a prime integer d from 2 to $\sqrt{g}$ that evenly divides g (the division leaves no remainder).
As sone as g is evenly divisible by d then g is composite, otherwise g is a prime number.

In the prime spiral with **one** segment each integer g is a unique member of the family of quadratic functions $f_{a,b,c}(n) = f_{1,b,c}(n) = f_{1,c}(n_E) = 1n^2 + 0n + c = n^2 + c$ with $-n < c \leq n$. This specific function has only two terms.
So, each integer g is defined as $g = n^2 + c$ with $-n < c \leq n$ and $n = \lfloor \sqrt{g} \rceil$.

The modulo primality test reduces the integer $g = n^2 + c$ into $g' = n' \cdot n' + c$ with $n' = n \pmod{d}$.
When there is a divisor d in $2 \leq d \leq \sqrt{g}$ with $g' \pmod{d} = 0$ then g is composite, otherwise g is a prime number.

The modulo primality test takes more operations than the straightforward division of the integer g by the divisors (appendix C: "Modular arithmetic").
The strength of the modulo primality test lies in the reduction of the size of the integer g (Fig. 2).

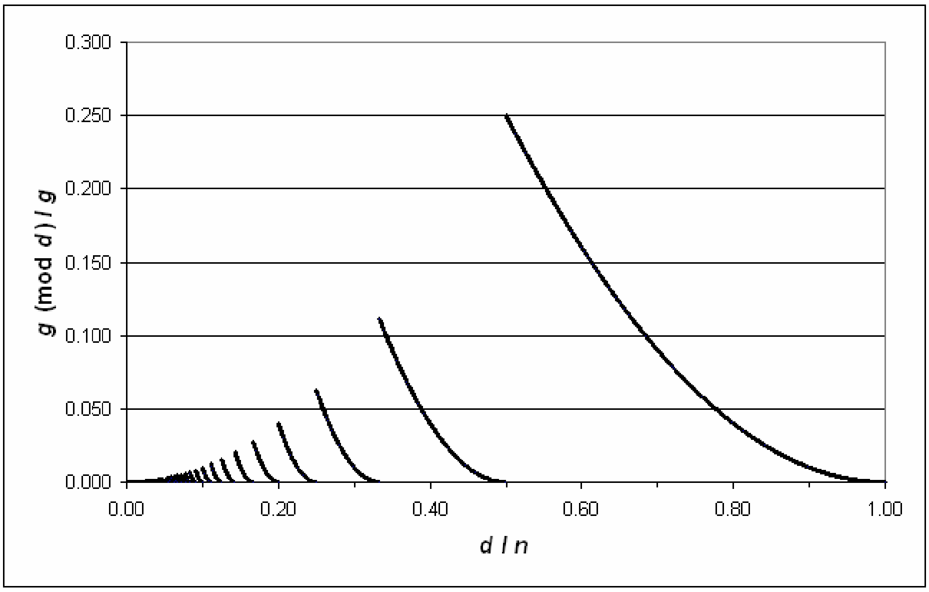

Fig. 2: The reduction of a integer as function of the divisor d via modular arithmetic.

Fig. 2 shows that the reduction of $\frac{g \pmod{d}}{g}$ bounces back to $\left(\frac{1}{m}\right)^2$ at every $\frac{d}{n} = \frac{1}{m}$ with $m \in \{ ..., 5, 4, 3, 2\}$.

From $\frac{1}{m+1}$ towards $\frac{1}{m}$ the value of $n' = n \pmod{d}$ slowly approaches zero via a quadratic function.

Further reduction of $g' \pmod{d} / g$ can be obtained by selective changing $n^2 = n \cdot n \equiv n' \cdot n' \pmod{d}$ into $n^2 = n \cdot n \equiv n' \cdot (n' - d) \pmod{d}$.

4. The modulo primality test to find verify large primes.

In the prime number theorem the prime-counting function $\pi(g)$ for the positive integers up to g is defined as:

$$\pi(g) \approx \frac{g}{\log(g)}$$ with $\log(g)$ the natural logarithm of g.

For large enough g, the probability that a random integer not greater than g is prime is close to $1 / \log(g)$.
Among the positive integers $g \approx 10^9$ about one in 21 is prime, since $\log(10^9) \approx 20.7$.
For prime numbers ≈ 10^10^8, about one in $2.3 \cdot 10^8$ is prime, since log(10^10^8) $= 10^8 \cdot \log(10) \approx 2.3 \cdot 10^8$.

The modulo primality test can be deployed to search for ever larger prime numbers, like the first prime number with at least one hundred million digits when written in base 10.
Below is a describtion of how to find the first prime number after integer g_s with the modulo primality test.

Imagine trying to find the first prime number after the integer g_s = 10^10^8 − 1

1. The prime spiral with one segment defines the integer g_s as member of $f_{1,c}(n_E) = n^2 + c$ with $-n < c \leq n$.
   Calculate both $n = \lfloor \sqrt{g} \rceil$ and $c = g - n^2$.
2. Take a list of prime numbers up to for instance $p_{end} = p_{238}$. Define $p_i \in \{p_2, ..., p_{end}\}$ thus $p_i \in \{3, ..., 1499\}$.
   Other options are:
   The $P_6\#$−sieve gives a list of all $\pi(p_6\#) = 3{,}248$ prime numbers $< p_6\#$ with $p_6\# = 30{,}030$.
   The extended $P_9\#$−sieve supplies a list of all prime numbers up to 10^9.
3. Calculate $g_s \pmod{p_i}$ for every given p_i via $g_s'(p_i) = (n' \cdot n' + c) \pmod{p_i}$ with $n' = n \pmod{p_i}$.
   Store the calculations of $g_s'(p_i)$ in an array.
4. Select the next odd integer g_v, with $\Delta g = g_v - g_s$ the distance between g_s and g_v.
   Calculate $g_v'(p_i) = (g_s'(p_i) + \Delta g) \pmod{p_i}$ for every given p_i up to p_{end}. Overwrite $g_s'(p_i)$ with $g_v'(p_i)$.
   As sone as $g_v' = 0$ then g_v is not a prime number. Repeat step 4.
5. When $g_v' \neq 0$ for every given p_i up to p_{end} then g_v could be a prime number.
   Use modular arithmetic (appendix C) to check g_v for primality.
   For instance with the $P_4\#$−sieve the division by the prime divisors $p_{end} < d < \sqrt{g_v}$ can be approximated by $d \in \{ S(p_4\#)_j + k \bullet p_4\# \mid 1 \leq j \leq \varphi(p_4\#) \wedge k \in \mathbf{N}_0 \}$ (see Appendix B).

5. The modulo primality test and RSA cryptography.

RSA cryptography is based on two large prime numbers g_A and g_B to generate a composite number $g = g_A \cdot g_B$. Multiplying the two large numbers g_A and g_B is easy. Factoring the large number g is very difficult.

For example, the RSA-100 number is defined as the semi-prime $g = 0.15226... \cdot 10^{100}$, the product of the prime numbers $g_A = 0.37975... \cdot 10^{50}$ and $g_B = 0.40094... \cdot 10^{50}$.
For demonstration purposes the RSA-100 number is replaced by the semi-prime $g = 1{,}523{,}012{,}791 = 0.15230... \cdot 10^{10}$ and the prime numbers $g_A = 0.37987 \cdot 10^5$ and $g_B = 0.40093 \cdot 10^5$.

Out of the infinite set of primorial sieves, the $P_4\#$–sieve is implemented with $p_4\# = 210$ and $\varphi(p_4\#) = 48$.
The integer $g = 1{,}523{,}012{,}791 \equiv 181 \pmod{p_4\#}$ could be prime since $181 = S(p_4\#)_{41}$ (see Appendix B).

The segmented prime spiral with one segment splits g into the two terms of the Eastward quadratic polynomial.
The function $f_{1,c}(n_E) = n^2 + c$ with $-n < c \leq n$ gives $n = \lfloor \sqrt{g} \rceil = 39{,}026$ and $c = -15{,}885$.
Find $d \mid g$ via $g = n \cdot n - 15{,}885 \equiv n' \cdot n' - 15{,}885 \pmod{d}$ with $n' \equiv n \pmod{d}$.

Possible divisors $p_4 < d < \sqrt{g}$ are $d \in \{ S(p_4\#)_j + k \cdot p_4\# \mid 1 \leq j \leq \varphi(p_4\#) \wedge k \in \mathbf{N}_0 \}$, based on the fourth double primorial sieve. Start at the end and work backwards, since the principles of RSA crytograhpy define $g = g_A \cdot g_B$ with $g_A \approx g_B \approx \sqrt{g} \approx n$.

$d \leq n$	$S(p_4\#)_j$	$n = 39{,}026$ $n' = n \pmod{d}$	$f_{1,-15885}(n_E) = n^2 - 15{,}885 = 1{,}523{,}012{,}791$ $f_{1,0,-15885}(39{,}026) \equiv n' \cdot n' - 15{,}885 \pmod{d}$	Comment about g
39,023	173	3	$3^2 - 15{,}885 \equiv -15{,}876 \quad - -\mathbf{1} \cdot d \equiv 23{,}147$	possible prime
39,019	169	7	$7^2 - 15{,}885 \equiv -15{,}836 \quad - -\mathbf{1} \cdot d \equiv 23{,}183$	possible prime
39,017	167	9	$9^2 - 15{,}885 \equiv -15{,}804 \quad - -\mathbf{1} \cdot d \equiv 23{,}213$	possible prime
. . .				
38,027	17	999	$999^2 - 15{,}885 \equiv 982{,}116 \quad - \mathbf{25} \cdot d \equiv 31{,}441$	possible prime
38,023	13	1,003	$1{,}003^2 - 15{,}885 \equiv 990{,}124 \quad - \mathbf{26} \cdot d \equiv 1{,}526$	possible prime
. . .				
37,997	197	1,029	$1{,}029^2 - 15{,}885 \equiv 1{,}042{,}956 \quad - \mathbf{27} \cdot d \equiv 17{,}037$	possible prime
37,993	193	1,033	$1{,}033^2 - 15{,}885 \equiv 1{,}051{,}204 \quad - \mathbf{27} \cdot d \equiv 25{,}393$	possible prime
37,991	191	1,035	$1{,}031^2 - 15{,}885 \equiv 1{,}055{,}340 \quad - \mathbf{27} \cdot d \equiv 29{,}583$	possible prime
37,987	187	1,039	$1{,}039^2 - 15{,}885 \equiv 1{,}063{,}636 \quad - \mathbf{28} \cdot d \equiv 0$ ◄	**NOT** prime

The "modulo primality test" claims: **Divisions? Who needs divisions!**

Based on the modulo primality test the RSA-100 number is reduced to maximum 0.001 of its original size.
This corresponds with fig. 2, since $\frac{d}{n} = \frac{g_A}{n} = \frac{0.37975... \cdot 10^{50}}{0.39020... \cdot 10^{50}} = 0.973....$

The modulo primality test uses the operations multiplication, adding, substracting and some fancy bookkeeping.
The division operation is not required, as shown in the table above. Appendix D gives an RSA-120 example.

References.

[1] Gardner, M. (1971). *Martin Gardner's Sixth Book of Mathematical Diversions from Scientific American*, University of Chicago Press

[2] Stein, M. L., Ulam, S. M & Wells, M. B. (1964). A visual display of some properties of the distribution of primes. *American Mathematical Monthly* 71:516–520.

[3] Wells, David (2011), *Prime Numbers: The Most Mysterious Figures in Math*, John Wiley & Sons

[4] Dicker, Hans (2013), *The (double) Primorial sieve* (http://www.primorial-sieve.com/_Primorial_sieve En.pdf)

[5] Dicker, Hans (2017), *The Ulam spiral unraveled* (http://www.primorial-sieve.com/_Ulam spiral unraveled.pdf)

Appendix A: The Ulam spiral unraveled.

The segmented prime spiral is a way to visualize the distribution of prime numbers amongst a sequential set of natural numbers. The segmented prime spiral consists of segments of sequential natural numbers, who together with other segments form a continuous spiral of natural numbers. There are infinitely many segmented prime spirals.

A counterclockwise prime spiral with startvalue 0 and m segments is fully defined by the $(2m + 1)$ families of quadratic functions $f_{a,b,c}(n) = an^2 + bn + c$, with $n \in N_0$, $m \in N$, $a = m$, $-a \leq b \leq a$ with $b \in Z$, and

$$\begin{cases} c \in Z_0^- & \text{if } b = a \\ c \in Z & \text{if } -a < b < a \\ c \in Z^+ & \text{if } b = -a \end{cases}$$

The Ulam spiral, as discovered by Stanislaw Ulam in 1963, is the most famous seqential prime spiral and has four segments. In the Ulam spiral prime numbers have the tendency to line up along specific odd diagonals, while other odd diagonals hardly contain any prime numbers. These clear patterns continue even when the spiral grows bigger.
The Ulam spiral can start with the initial value 1 as used by Ulam (Fig. A.1), or with any other natural number.

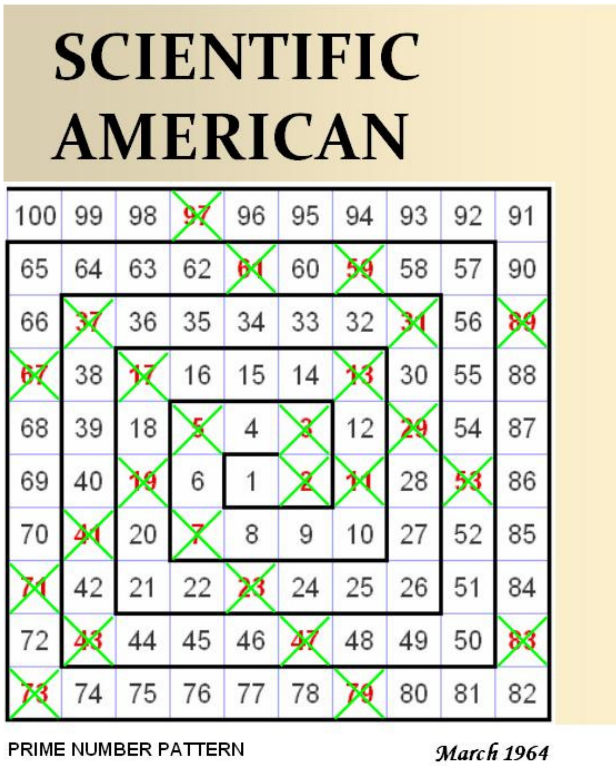

Fig. A.1: Ulam's spiral on the cover of Scientific American, March 1964.

Placing the Ulam spiral with startvalue 0 in a Cartesian coordinate system reveals the location of any integer by way of n and c (Fig. A.2).

The Ulam spiral is a four quarter prime spiral. At the SE main diagonal the family of functions changes from $f_c(n_{\mathrm{SE(S)}}) = 4n^2 + 4n + c$ with $c \in Z_0^-$ into $f_c(n_{\mathrm{SE(E)}}) = 4n^2 - 4n + c$ with $c \in Z^+$.
When separating the four segments, integers on the seam appear twice due to the translation $n \longmapsto n - 1$ (Fig. A.3).

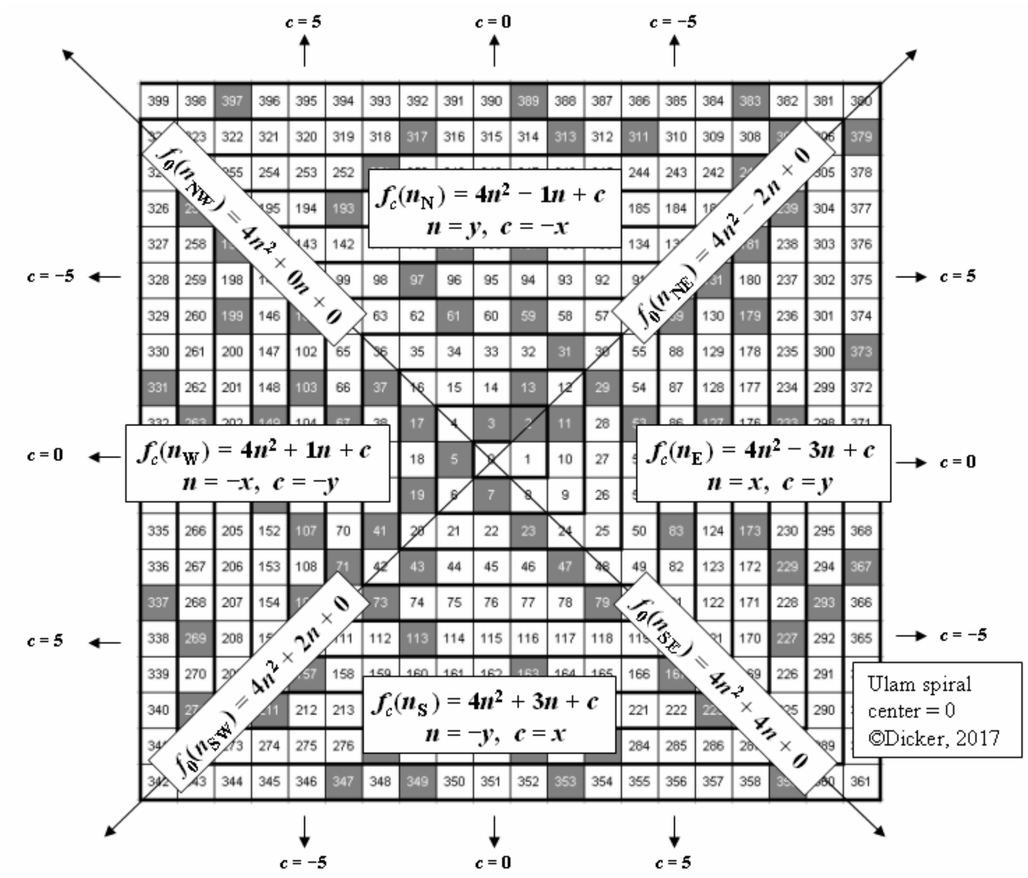

Fig. A.2: The Ulam spiral and the $(2m + 1)$ families of functions, with $m = 4$.

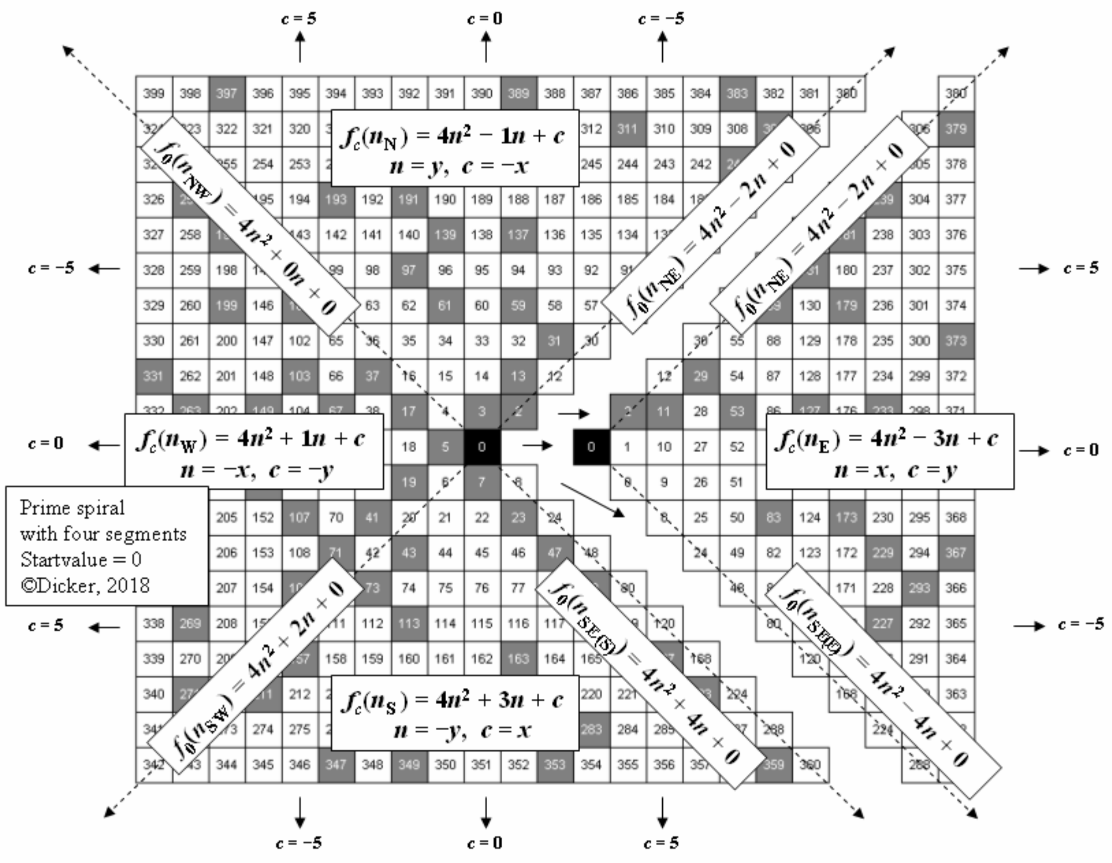

Fig. A.3: Visualization of the four segments of the Ulam spiral with startvalue 0.

Appendix B: The (double) primorial sieve.

The primorial sieve consists of the infinite set $P_n\#$–sieves, thus the $P_1\#$–sieve, $P_2\#$–sieve, ... , $P_n\#$–sieve.
Each sieve is derived from the previous sieve.
The width of the sieve is equal to the primorial $p_n\#$, the product of the first n prime numbers. All natural numbers sequential arranged on top of the base of the sieve form together a matrix of infinite height.
The $\varphi(p_n\#)$ struts $S(p_n\#)_j$ of the sieve support the columns above which potential prime numbers $g > p_n$ are located, that comply with $g \pmod{p_n\#} \in \{ S(p_n\#)_j \mid 1 \le j \le \varphi(p_n\#) \}$ and $\varphi(p_n\#)$ Euler's totient function.
Non-prime numbers $> p_n$ with $gcd\,(g,\ p_n\#) \ne 1$ are filtered through holes in the sieve.
From the $P_4\#$–sieve onwards struts can be composite numbers.

The **double** primorial sieve is a method for preliminary filtering of potential prime numbers within all natural numbers.
Of the infinite set of natural numbers $> p_n$ only $\varphi(p_n\#)\ /\ p_n\#$ could be a prime number.
For the final check of a potential prime number $g > p_n$ the division by prime divisors $d < \sqrt{g}$ can be approximated by $d \in \{ S(p_n\#)_j + k \bullet p_n\# \mid 1 \le j \le \varphi(p_n\#) \wedge k \in \mathbf{N}_0 \}$.

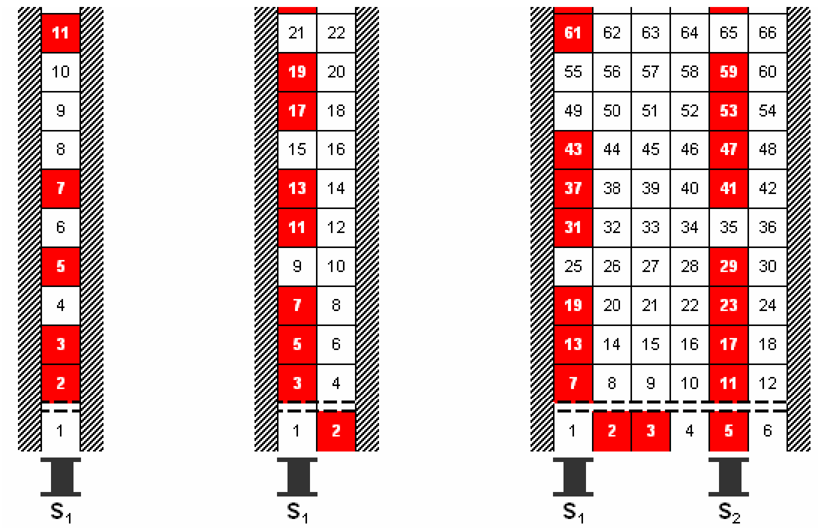

Fig. B.1abc: The double primorial sieves: $P_0\#$–sieve, $P_1\#$–sieve and $P_2\#$–sieve.

The $P_0\#$–sieve is the startingpoint to build ever increasing sieves. Formally the $P_0\#$–sieve does not exist, since $p_0 = 1$ is not a prime number. All integers are above the S_1 strut, there is no filtering (Fig. B.1a).
The $P_1\#$–sieve is p_1 times wider than the $P_0\#$–sieve and selects odd integers $> p_1$ as possible prime numbers.
In the $P_2\#$–sieve only integers $> p_2$ that comply with $(6k \pm 1)$ could be prime numbers (Fig. B.1bc).

Every $P_n\#$–sieve contains a list of all prime numbers $< p_n\#$. The list consist out of the prime numbers $\le p_n$ and the struts > 1 that are not composite numbers.

The $P_9\#$–sieve with a base of $p_9\# = 223{,}092{,}870$ and $\varphi(p_9\#) = 36{,}495{,}360$ struts, is the last sieve where 4 Byte integers suffice in computer calculations .

The $P_3\#$–sieve has a width of $p_3\# = p_3 \bullet p_2\# = 30$ and $\varphi(p_3\#) = 8$ struts. The $P_3\#$–sieve provides the list of prime numbers $< p_3\#$ consisting of the prime numbers $p_i \in \{2, 3, 5\}$ and the struts S_j that satisfy $gcd\,(S_j,\ p_3\#) = 1$ with $1 < j \leq \varphi(p_3\#)$. Note that with the third primorial sieve all struts > 1 are prime numbers. Potential prime numbers $> p_3\#$ are situated above the struts and meet both $gcd\,(g,\ p_3) = 1$ and $gcd\,(g,\ p_3\#) = 1$ (Fig. B.2a).

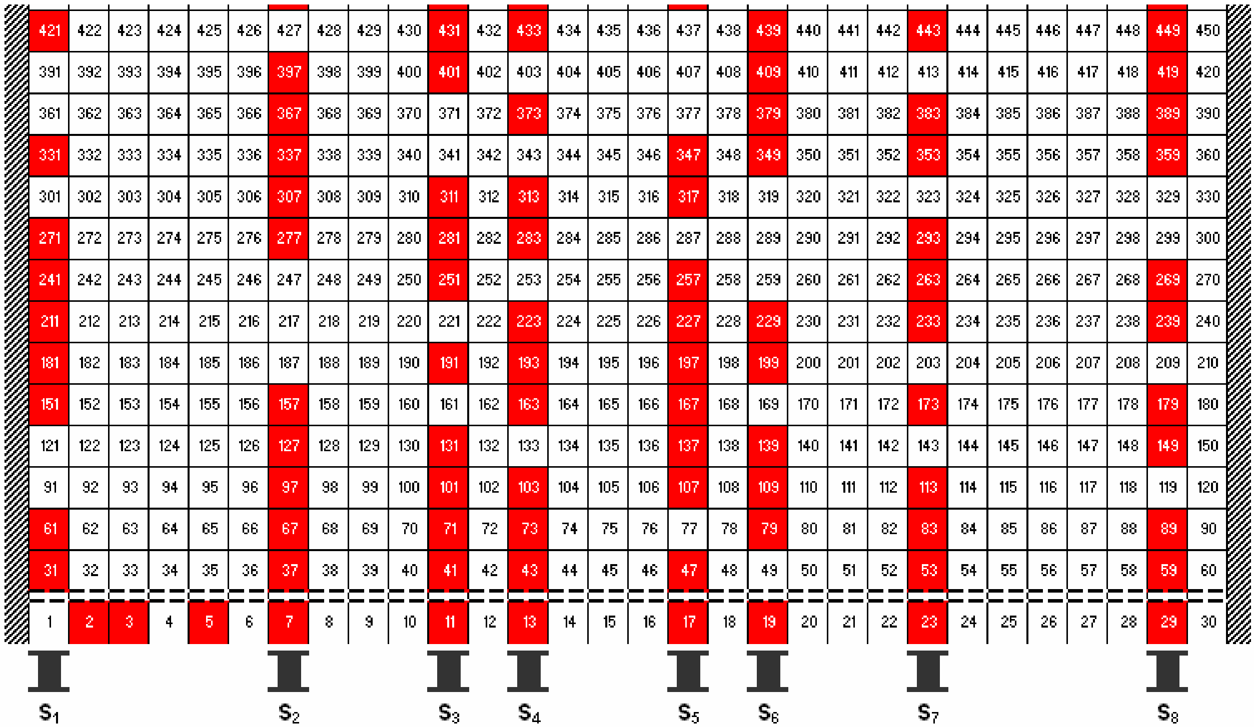

Fig. B.2a: The third double primorial sieve.

The $P_3\#$–sieve has many similarities with the Wheel Factorization method of Paul Pritchard. Fig. B2b shows a wheel with the inner circle formed by the first 30 natural numbers, and thus with a $p_3\# = 30$ base. The spokes of the wheel that contain possible prime numbers have the same functionality as the columns above the struts of the primorial sieve.
The graphical representation of the wheel is in this case more concrete. Clearly visible is the symmetry of the spokes in $p_3\# / 2$.

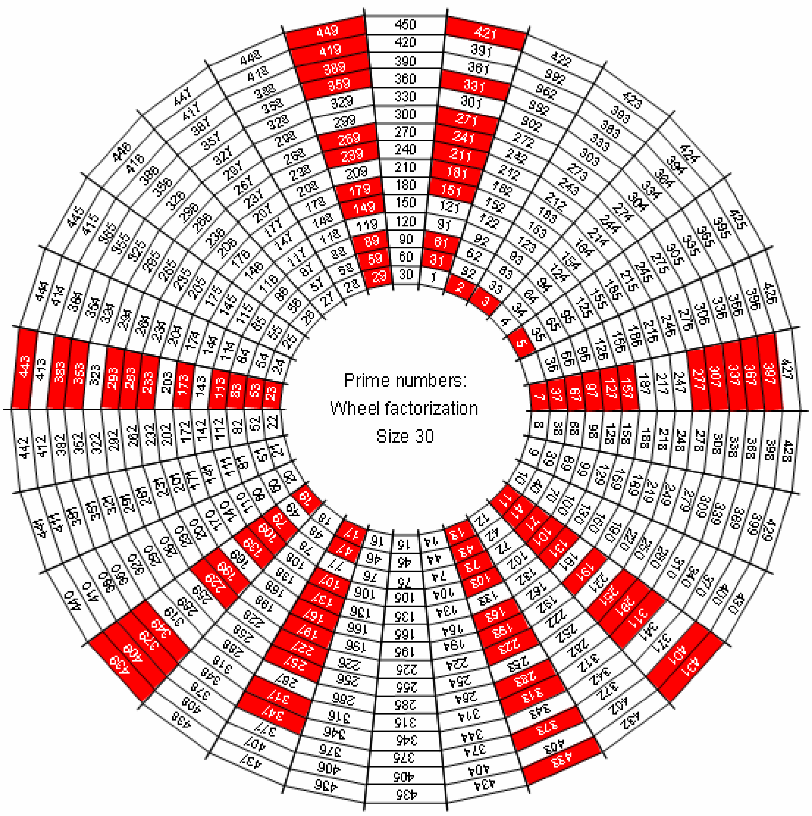

Fig. B.2b: Wheel factorization with size 30.

From the $P_4\#$−sieve onwards the struts could be composite numbers.
To generate the list $> p_4$ with all prime numbers $< p_4\#$ from the struts of the $P_4\#$−sieve the composite struts $S(p_4\#)_j$ with $j \in \{28, 33, 39, 43, 48\}$ are marked negative (Fig. 3).
These composite struts are found via $S(p_4\#)_j \bullet S(p_4\#)_i < p_4\#$ with $i, j > 1$ and $S(p_4\#)_j \le S(p_4\#)_i$.
Thus: **11** • 11 = 121, **11** • 13 = 143, **11** • 17 = 187, **11** • 19 = 209 and **13** • 13 = 169.
The prime numbers $\le p_4$ plus the non-composite struts $> p_4$ supply the list of the 46 prime numbers $< p_4\#$.

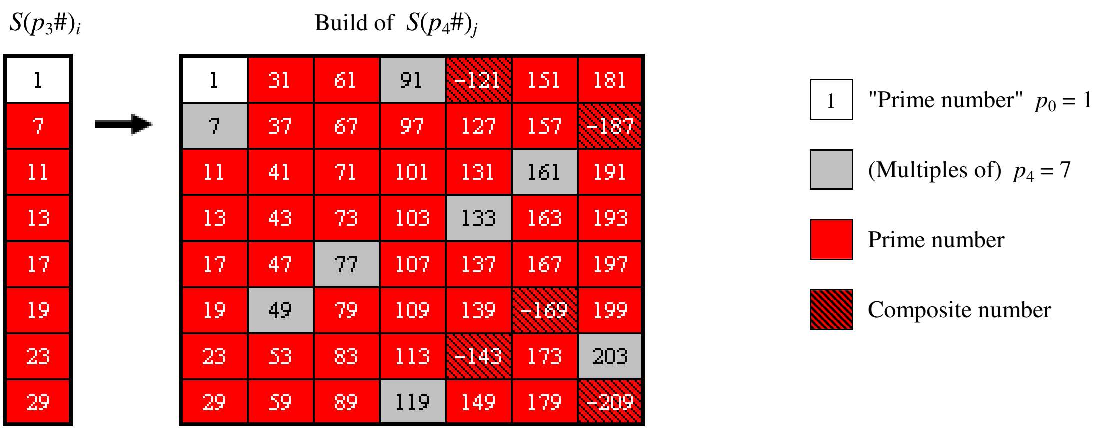

Fig. B.3: The $\varphi(p_4\#) = 48$ struts of the $P_4\#$−sieve build out of the $P_3\#$−sieve.

Fig. B.4 shows the equal distribution of the $\pi(10^9) = 50{,}847{,}534$ prime numbers above the struts of the $P_4\#$−sieve, with a deviation relative to $\pi(10^9) / \varphi(p_4\#)$ of less than 0.05%. Among the $\varphi(p_4\#) = 48$ struts of the $P_4\#$−sieve the influence is still visible of the repeated pattern of the 8 struts $S_i \in \{1, 7, 11, 13, 17, 19, 23, 29\}$ of the $P_3\#$−sieve.
The distance ΔS between S_1 and S_2 of the $P_4\#$−sieve is equal to $\Delta S = S(p_4\#)_2 - S(p_4\#)_1 = p_5 - p_0 = 11 - 1 = 10$.
This gap is the biggest gap between struts. Due to the symmetry in $(p_4\# / 2)$ the distance ΔS is also found between the second to last and the last strut of the sieve.

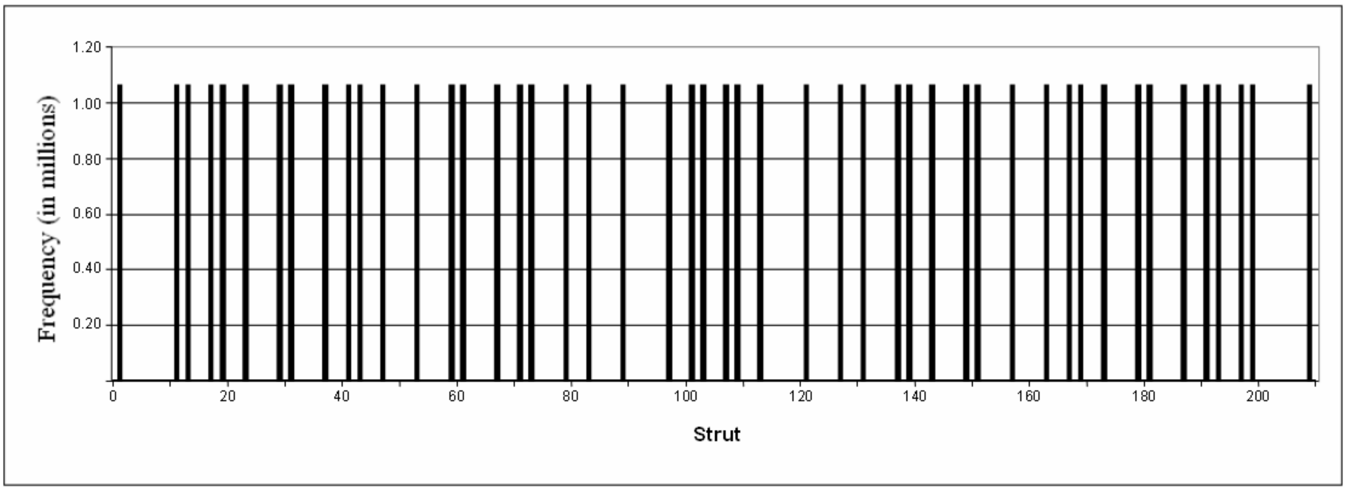

Fig. B.4: $P_4\#$−sieve: equal distribution of prime numbers $< 10^9$ above the 48 struts, with $\pi(10^9) = 50{,}847{,}534$.

Appendix C: Modular arithmetic.

Example 1: given integer $g_1 = 1{,}003{,}242{,}049$ is a "very large" integer.

Test the integer g_1 via the Primorial sieve, for instance the fourth primorial sieve with $p_4\# = 210$.
The $P_4\#$-Sieve has $\varphi(p_4\#) = 48$ struts S_j with $1 \le j \le \varphi(p_4\#)$ and $gcd\,(S_j,\ p_4\#) = 1$.
The "very large" integer $g_1 \equiv 19 \pmod{p_4\#}$ could be prime since $19 = S_5$.
Possible divisors $p_4 < d < \sqrt{g_1}$ now are $d \in \{\ S(p_4\#)_j + k \cdot p_4\# \ \big|\ 1 \le j \le \varphi(p_4\#) \wedge k \in \mathbf{N}_0\ \}$, based on the fourth double primorial sieve (appendix B).

The segmented prime spiral with one segment splits g_1 into the two terms of the Eastward quadratic polynomial.
The function $f_{1,c}(n_E) = 1n^2 + 0n + c = n^2 + c$ with $-n < c \le n$ gives $n = \lfloor \sqrt{g_1} \rceil = 31{,}674$ and $c = -227$.

Modular arithmetic is now used to check if $g_1 \equiv 1{,}003{,}242{,}049 \pmod d$ is a prime number.
Thus $f_{1,\,-227}(n_E) = n \cdot n - 227 \equiv n' \cdot n' - 227 \pmod d$ with $n' \equiv n \pmod d$.

$d \le n$	$S(p_4\#)_j$	$n = 31{,}674$ $n' = n \pmod d$	$f_{1,-227}(n_E) = n \cdot n - 227 = 1{,}003{,}242{,}049$ $f_{1,0,-227}(31{,}674) \equiv n' \cdot n' - 227 \pmod d$	Comment about g_1
11	11	5	$5^2 - 227 \equiv -202 + \mathbf{19} \cdot d \equiv 7$	possible prime
13	13	6	$6^2 - 227 \equiv -191 + \mathbf{15} \cdot d \equiv 4$	possible prime
17	17	3	$3^2 - 227 \equiv -218 + \mathbf{17} \cdot d \equiv 3$	possible prime
. . .				
1,501	31	153	$153^2 - 227 \equiv 23{,}182 - \mathbf{15} \cdot d \equiv 667$	possible prime
1,507	37	27	$27^2 - 227 \equiv 502 - \mathbf{0} \cdot d \equiv 502$	possible prime
1,511	41	1,454	$1{,}454^2 - 227 \equiv 2{,}113{,}889 - \mathbf{1{,}399} \cdot d \equiv 0$ ◄	**NOT** prime

Example 2: given integer $g_2 = 1{,}006{,}824{,}671$ is a "very large" integer.

The integer $g_2 \equiv 41 \pmod{p_4\#}$ could be prime since $41 = S_{10}$.
The function $f_{1,c}(n_E) = 1n^2 + 0n + c = n^2 + c$ with $-n < c \le n$ gives $n = \lfloor \sqrt{g_2} \rceil = n = 31{,}731$ and $c = -31{,}690$.

$d \le n$	$S(p_4\#)_j$	$n = 31{,}731$ $n' = n \pmod d$	$f_{1,-31690}(n_E) = n \cdot n - 31{,}690 = 1{,}006{,}824{,}671$ $f_{1,0,-31690}(31{,}731) \equiv n' \cdot n' - 31{,}690 \pmod d$	Comment about g_2
11	11	7	$7^2 - 31{,}690 \equiv -31{,}641 + \mathbf{2{,}877} \cdot d \equiv 6$	possible prime
13	13	11	$17^2 - 31{,}690 \equiv -31{,}569 + \mathbf{2{,}429} \cdot d \equiv 8$	possible prime
17	17	9	$9^2 - 31{,}690 \equiv -31{,}609 + \mathbf{1{,}860} \cdot d \equiv 11$	possible prime
. . .				
15,863	113	5	$5^2 - 31{,}690 \equiv -31{,}665 + \mathbf{2} \cdot d \equiv 61$	possible prime
15,871	121	15,860	$15{,}860^2 - 31{,}690 \equiv 251{,}507{,}910 - \mathbf{15{,}847} \cdot d \equiv 173$	possible prime
15,877	127	15,854	$15{,}854^2 - 31{,}690 \equiv 251{,}317{,}626 - \mathbf{15{,}829} \cdot d \equiv 593$	possible prime
. . .				
28,447	97	3,284	$3{,}284^2 - 31{,}690 \equiv 10{,}752{,}966 - \mathbf{378} \cdot d \equiv 0$ ◄	**NOT** prime

Example 3: given integer $g_3 = 1{,}012{,}576{,}099$ is a "very large" integer.

The integer $g_3 \equiv 199 \pmod{p_4\#}$ could be prime since $199 = S_{47}$.
The function $f_{1,c}(n_E) = 1n^2 + 0n + c = n^2 + c$ with $-n < c \le n$ gives $n = \lfloor \sqrt{g_3} \rceil = 31{,}821$ and $c = 58$.

$d \le n$	$S(p_4\#)_j$	$n = 31{,}821$ $n' = n \pmod d$	$f_{1,58}(n_E) = n^2 + 58 = 1{,}012{,}576{,}099$ $f_{1,0,58}(31{,}821) \equiv n' \cdot n' + 58 \pmod d$	**Comment about g_3**
11	11	9	$9^2 + 58 \equiv 139 - \mathbf{12} \cdot d \equiv 7$	possible prime
13	13	10	$10^2 + 58 \equiv 158 - \mathbf{2{,}448} \cdot d \equiv 1$	possible prime
17	17	14	$14^2 + 58 \equiv 254 - \mathbf{1{,}872} \cdot d \equiv 1$	possible prime
. . .				
15,907	157	7	$7^2 + 58 \equiv 107 - \mathbf{0} \cdot d \equiv 107$	possible prime
15,913	163	15,908	$15{,}908^2 + 58 \equiv 253{,}064{,}522 - \mathbf{15{,}903} \cdot d \equiv 83$	possible prime
15,917	167	15,904	$15{,}904^2 + 58 \equiv 252{,}937{,}274 - \mathbf{15{,}891} \cdot d \equiv 227$	possible prime
. . .				
31,819	109	2	$2^2 + 58 \equiv 62 - \mathbf{0} \cdot d \equiv 62$	**Prime**
31,823	113			$d \ge \sqrt{g_3}$ ▲

Example 4: given integer $g_4 = 1{,}012{,}862{,}449$ is a "very large" integer.

The integer $g_4 \equiv 109 \pmod{p_4\#}$ could be prime since $109 = S_{26}$.
The function $f_{1,c}(n_E) = 1n^2 + 0n + c = n^2 + c$ with $-n < c \le n$ gives $n = \lfloor \sqrt{g_3} \rceil = 31{,}825$ and $c = 31{,}824$.

$d \le n$	$S(p_4\#)_j$	$n = 31{,}825$ $n' = n \pmod d$	$f_{1,31824}(n_E) = n^2 + 31{,}824 = 1{,}012{,}862{,}449$ $f_{1,0,31824}(31{,}825) \equiv n' \cdot n' + 31{,}824 \pmod d$	**Comment about g_4**
11	11	2	$2^2 + 31{,}824 \equiv 31{,}828 - \mathbf{2{,}893} \cdot d \equiv 5$	possible prime
13	13	1	$1^2 + 31{,}824 \equiv 31{,}825 - \mathbf{2{,}448} \cdot d \equiv 1$	possible prime
17	17	1	$1^2 + 31{,}824 \equiv 31{,}825 - \mathbf{1{,}872} \cdot d \equiv 1$	possible prime
. . .				
[1] 15,907	157	11	$11^2 + 31{,}824 \equiv 31{,}945 - \mathbf{2} \cdot d \equiv 131$	possible prime
[2] 15,913	163	15,912	$15{,}912^2 + 31{,}824 \equiv 253{,}223{,}568 - \mathbf{15{,}909} \cdot d \equiv 15{,}912$	possible prime
[3] 15,917	167	15,908	$15{,}908^2 + 31{,}824 \equiv 253{,}096{,}288 - \mathbf{15{,}901} \cdot d \equiv 71$	possible prime
. . .				
31,823	113	2	$2^2 + 31{,}824 \equiv 31{,}828 - \mathbf{1} \cdot d \equiv 5$	**Prime**
31,831	121			$d \ge \sqrt{g_4}$ ▲

Reducing the cpu-power needed.

Every calculation for the next d can be based on results of the previous step.
For instance $d_{old} = 15{,}907$ gives $n'_{old} = 11 \pmod{d_{old}}$ and $f_{1,0,31825}(n_E) \equiv n'_{old} \cdot n'_{old} + 31{,}824 \equiv 31{,}945$, see note [1].
Define $g'_{old}(n'_{old}) = g'_{old}(11) = n'_{old} \cdot n'_{old} + 31{,}824 = 31{,}945$, see note [2].
Then $d_{new} = 15{,}913$ gives $n'_{new} = 15{,}912 \pmod{d_{new}}$ and $\Delta n' = n'_{new} - n'_{old} = 15{,}901$
Now $g'_{new}(n'_{new}) = n'_{new} \cdot n'_{new} + 31{,}824$
$= (n'_{old} + \Delta n') \cdot (n'_{old} + \Delta n') + 31{,}824$
$= g'_{old}(n'_{old}) + 2 \cdot n'_{old} \cdot \Delta n' + (\Delta n')^2$
$= g'_{old}(n'_{old}) + (n'_{old} + n'_{old} + \Delta n') \cdot \Delta n'$
$= 31{,}945 + (11 + 11 + 15{,}901) \cdot 15{,}901 = 253{,}223{,}568$.
Next step: $g'_{old}(n'_{old}) = 253{,}223{,}568$ with $n'_{old} = 15{,}912$, see previous step
Then $d_{new} = 15{,}917$ gives $n'_{new} = 15{,}908 \pmod{d_{new}}$ and $\Delta n' = n'_{new} - n'_{old} = -4$
Now $g'_{new}(n'_{new}) = g'_{old}(n'_{old}) + (n'_{old} + n'_{old} + \Delta n') \cdot \Delta n'$
$= 253{,}223{,}568 + (15{,}912 + 15{,}912 + -4) \cdot -4 = 253{,}096{,}228$, see note [3].

Appendix D: Example of how to factorize the RSA-120 number.

RSA cryptography is based on two large prime numbers g_A and g_B to generate a composite number $g = g_A \cdot g_B$. Multiplying the two large numbers g_A and g_B is easy. Factoring the large number g is very difficult.

The RSA-120 number is defined as the semi-prime $g = 0.22701... \cdot 10^{120}$, the product of the prime numbers $g_A = 0.32741... \cdot 10^{60}$ and $g_B = 0.69334... \cdot 10^{60}$.
For demonstration purposes the RSA-120 number is replaced by the semi-prime $g = 2{,}270{,}717{,}413 = 0.22707... \cdot 10^{10}$ with the prime numbers $g_A = 0.32749 \cdot 10^5$ and $g_B = 0.69337 \cdot 10^5$.

The segmented prime spiral with one segment splits g into the two terms of the Eastward quadratic polynomial.
So $g = f_{1,c}(n_E) = n^2 + c$ with $-n < c \le n$ gives $n = \lfloor \sqrt{g} \rceil = 47{,}652$ and $c = 4{,}309$.
Find $d \mid g$ via $g = n \cdot n + 4{,}309 \equiv n' \cdot n' + 4{,}309 \pmod{d}$ with $n' \equiv n \pmod{d}$.

Possible divisors $p_4 < d < \sqrt{g}$ are $d \in \{ S(p_4\#)_j + k \cdot p_4\# \mid 1 \le j \le \varphi(p_4\#) \wedge k \in \mathbf{N}_0 \}$, based on the fourth double primorial sieve. Start at the end and work backwards, since the principles of RSA crytograhpy define $g = g_A \cdot g_B$ with $g_A \approx g_B \approx \sqrt{g} \approx n$.

$d \le n$	$S(p_4\#)_j$	**$n = 47{,}652$** **$n' = n \pmod{d}$**	**$f_{1,4309}(n_E) = n^2 + 4{,}309 = 2{,}270{,}717{,}413$** **$f_{1,0,4309}(47{,}652) \equiv n' \cdot n' + 4{,}309 \pmod{d}$**	**Comment about g**
47,651	191	1	$1^2 + 4{,}309 \equiv 4{,}310 - \mathbf{0} \cdot d \equiv 4{,}310$	possible prime
47,647	187	5	$5^2 + 4{,}309 \equiv 4{,}334 - \mathbf{0} \cdot d \equiv 4{,}334$	possible prime
47,641	181	11	$11^2 + 4{,}309 \equiv 4{,}430 - \mathbf{0} \cdot d \equiv 4{,}430$	possible prime
. . .				
32,791	31	14,861	$14{,}861^2 + 4{,}309 \equiv 220{,}853{,}630 - \mathbf{6{,}735} \cdot d \equiv 6{,}245$	possible prime
32,789	29	14,863	$14{,}863^2 + 4{,}309 \equiv 220{,}913{,}078 - \mathbf{6{,}737} \cdot d \equiv 13{,}585$	possible prime
32,783	23	14,869	$14{,}869^2 + 4{,}309 \equiv 221{,}091{,}470 - \mathbf{6{,}744} \cdot d \equiv 2{,}918$	possible prime
32,779	19	14,873	$14{,}873^2 + 4{,}309 \equiv 221{,}210{,}438 - \mathbf{6{,}748} \cdot d \equiv 17{,}746$	possible prime
32,777	17	14,875	$14{,}875^2 + 4{,}309 \equiv 221{,}269{,}934 - \mathbf{6{,}750} \cdot d \equiv 25{,}184$	possible prime
32,773	13	14,879	$14{,}879^2 + 4{,}309 \equiv 221{,}388{,}950 - \mathbf{6{,}755} \cdot d \equiv 7{,}335$	possible prime
32,771	11	14,881	$14{,}881^2 + 4{,}309 \equiv 221{,}448{,}470 - \mathbf{6{,}757} \cdot d \equiv 14{,}823$	possible prime
32,761	1	14,891	$14{,}891^2 + 4{,}309 \equiv 221{,}746{,}190 - \mathbf{6{,}768} \cdot d \equiv 19{,}742$	possible prime
1) 32,759	209	14,893	$14{,}893^2 + 4{,}309 \equiv 221{,}805{,}758 - \mathbf{6{,}770} \cdot d \equiv 27{,}328$	possible prime
2) 32,749	199	14,903	$14{,}903^2 + 4{,}309 \equiv 222{,}103{,}718 - \mathbf{6{,}782} \cdot d \equiv 0$ ◄	**NOT** prime

Every calculation for the next d can be based on results of the previous step to reduce the cpu-power needed.

For instance $d_{old} = 32{,}759$ gives $n'_{old} = 14{,}893 \pmod{d_{old}}$ and $f_{1,4309}(n_E) \equiv n'_{old} \cdot n'_{old} + 4{,}309 \equiv 221{,}805{,}758$, see note 1).
Define $g'_{old}(n'_{old}) = n'_{old} \cdot n'_{old} + 4{,}309$
Then $d_{new} = 32{,}749$ gives $n'_{new} = 14{,}903 \pmod{d_{new}}$ and $\Delta n' = n'_{new} - n'_{old} = 10$
Now
$$\begin{aligned} g'_{new}(n'_{new}) &= n'_{new} \cdot n'_{new} + 4{,}309 \\ &= (n'_{old} + \Delta n') \cdot (n'_{old} + \Delta n') + 4{,}309 \\ &= g'_{old}(n'_{old}) + 2 \cdot n'_{old} \cdot \Delta n' + (\Delta n')^2, \\ &= g'_{old}(n'_{old}) + (n'_{old} + n'_{old} + \Delta n') \cdot \Delta n', \end{aligned}$$
see note 2).

Define $r'_{old} = g'_{old}(n'_{old}) - m_{old} \cdot d_{old}$ with $0 \le r'_{old} < d_{old}$ and r the residue
Then $r'_{new} = g'_{new}(n'_{new}) - m_{new} \cdot d_{new}$ with $0 \le r'_{new} < d_{new}$.
$= (g'_{new}(n'_{new}) - m_{old} \cdot d_{new}) - \Delta m \cdot d_{new}$ with Δm found by repeated substractions.

The modulo primality test uses the operations multiplication, adding, substracting and some fancy bookkeeping. The division operation is not required, as shown in the table above.

Ergo: **Divisions? Who needs divisions!**

Appendix E: Summary.

Characteristics of the prime spiral with **one** segment.

A counterclockwise prime spiral with startvalue 0 and m segments is fully defined by the $(2m + 1)$ families of quadratic functions $f_{a,b,c}(n) = an^2 + bn + c$, with $n \in N_0$, $m \in N$, $a = m$, $-a \le b \le a$

with $b \in Z$, and
$$\begin{cases} c \in Z_0^- & \text{if } b = a \\ c \in Z & \text{if } -a < b < a \\ c \in Z^+ & \text{if } b = -a \end{cases}$$

The prime spiral with **one** segment has the 3 families of functions
$f_{1,b,c}(n) = 1n^2 + bn + c$ (see above)

The Eastward quadratic polynomial has the function
$f_{1,0,c}(n) = 1n^2 + 0n + c$ with $-n < c \le n$
or $f_{1,c}(n_E) = 1n^2 + c$

For any integer g applies
$g = f_{1,c}(n_E) = n^2 + c$ with $n = \lfloor \sqrt{g} \rceil$ and $c = g - n^2$

Modular arithmetics.

$g = n^2 + c = n \cdot n + c$ with $n = \lfloor \sqrt{g} \rceil$ and $c = g - n^2$
$g \equiv (n \cdot n + c) \pmod d \equiv (n \pmod d \cdot n \pmod d + c) \pmod d$
$g' \equiv (n' \cdot n' + c) \pmod d$ with $n' = n \pmod d$

Define $g'_{old}(n'_{old}) = n'_{old} \cdot n'_{old} + c$ based on $g \equiv (n_{old} \cdot n_{old} + c) \pmod{d_{old}}$
Then $g'_{new}(n'_{new}) = n'_{new} \cdot n'_{new} + c$
$= (n'_{old} + \Delta n') \cdot (n'_{old} + \Delta n') + c$ with $\Delta n' = n'_{new} - n'_{old}$
$= g'_{old}(n'_{old}) + 2 \cdot n'_{old} \cdot \Delta n' + (\Delta n')^2$
$= g'_{old}(n'_{old}) + (n'_{old} + n'_{old} + \Delta n') \cdot \Delta n'$

Checking for primality.

Given g is a large possible prime number.

Use the Primorial sieve:
Check g against the struts of the $P_n\#$–sieve
$g \pmod{p_n\#} \in \{ S(p_n\#)_j \mid 1 \le j \le \varphi(p_n\#) \}$
with $\varphi(p_n\#)$ Euler's totient function.
g is not a prime number if $gcd\,(g \pmod{p_n\#},\ p_n\#) \ne 1$

Use the **double** Primorial sieve:
Check g for primality via $d \mid g$ for $p_n < d < \sqrt{g}$
use $d \in \{ S(p_n\#)_j + k \bullet p_n\# \mid 1 \le j \le \varphi(p_n\#) \wedge k \in N_0 \}$
when no divisor is found, then g is a prime number