Cubic Groups

M. A. Popov

Abstract

Post-nonclassical intuitionistic “natural” arithmetic with its fundamental simplifications in the case of the problem of asymptotic distribution of primes is considered. It is showed that an existence of the cubic groups and n^3th density of prime distribution are assuming an existence of the one-way function of the form $f(x^3) = y, f^{-1}(y) = ?x^3$.

MSC2010 11Z99

TEXT

Let us imagine an existence of some kind of “natural arithmetic”, inspired by analogy with DNA's way to package an infinite number of points – mutations by just the two strands of the double helix. In other words, in contrast with invented human mathematics with its dogma of natural series [1] all the points ,or series of the natural numbers, of DNA – like intuitionistic arithmetics lie not on an intuitive straight line, but they lie on the two (odd – even) lines of some symmetrical figure. Thus, counter – intuitively, there are two strands here - “odd “ strand and “even” strand. Hence, immediately new fundamental simplifications and unexpected theorems are arising.

In particularly, fundamental problem of asymptotic distribution of primes could be understood as problem of distribution of primes among odd integers , needed a new kind of functions. Indeed, following Nicomachus theorem which assume that the *n*th cubic number n^3 is <u>a sum</u> of *n* consecutive odd numbers, all odd numbers of odd “strand “ can be self – organized into cubically bounded finite cubic groups :

2^3 = (3 + 5) **Rank 2 C^3Group**
3^3 = (7 + 9 +11) **Rank 3C^3 Group**
4^3 = (13 + 15 + 17+ 19) **Rank 4 C^3Group**
5^3 = (21 + 23 + 25 + 27 + 29) **Rank 5 C^3Group**
6^3 = (31 + 33 + 35 + 37 + 39 + 41) **Rank 6 C^3Group**
7^3 = (43 + 45 + 47 + 49 + 51 + 53 + 55) **Rank 7 C^3Group**,

generally, thus,

8^3 = (57, 59, 61, 63, 65, 67, 69, 71) **Rank 8 C^3Group**
9^3 = (73, 75, 77, 79, 81,83, 85, 87, 89) **Rank 9 C^3 Group**
10^3 = (91, 93, 95, 97, 99, 101, 103, 105, 107, 109) **Rank 10C^3Group**
11^3 = (111, 113, 115, 117, 119, 121, 123, 125,127, 129,131) **Rank 11 C^3 Group**
12^3 = (133, 135, 137, 139, 141,143, 145,147, 149, 151, 153, 155) **Rank 12 C^3Group**
13^3 = (157, 159, 161, 163, 165, 167, 169, 171, 173,175, 177, 179,181) **Rank 13 C^3 Group**
14^3 = (183,185,187,189, 191,193,195,197,199,201,203,205 207,209) **Rank 14 C^3Group**
15^3 = (211,213,215,217,219,221,223,225,227,229,231,233,235,237,239) **Rank 15 C^3 Group**
16^3 = (241,243,245,247,249,251,253,255,257,259,261,263,265,267,269,271) **Rank 16 C^3 Group**
17^3 = (273,275, 277,279,281,283,285,287,289,291,293,295,297,299,301,303,305) **Rank 17 C^3 Group**
18^3 = (307, 309,311,313,315,317,319, 321,323,325,327,329,331,333,335,337,339,341)**Rank 18 Group**
19^3 = (343,345,347,349,351,353,355,357,359,361,363,365,367,369,371,373,375,377,379) **Rank 19 C^3 Group**
20^3 = (381,383,385,387,389,391,393,395,397,399,401,403,405,407,409,411,413,415,417,419)**Rank20C^3Group**
etc...

where the n^3th length represents a kind of n^3th density of prime distribution.

Thus, in

2^3 - interval of odd strand there are 2 primes
3^3 - interval of odd strand there are 2 primes;
4^3 - interval of odd strand there are 3 primes;
5^3 - interval of odd strand there are 2 primes;
6^3 - interval of odd strand there are 3 primes;
7^3 - interval of odd strand there are 3 primes ;
…., etc

However, in order to express such form of functional inter -dependence we are needed a notion of one way function.

DEFINITION +. One way function is a function *f* from a set *x* to a set *y* if that is easy to compute for all $x \in X$, but hard to invert.[2][3].Their existence would prove that the computational complexity classes P and NP are distinct , correspondingly, complete test for all possible permutations (" perebor" in Levin's sense [2]) by "brutal force" is not avoidable. Examples of known hypothetical one way functions are : $x \rightarrow x^2 \mod n$ (where $n = prime \cdot prime$); $f^{\circ}(x_1,...x_n) = f(x_1) ... f(x_n)$, and, $D' = A^2QA$ [3].

Hence,

LEMMA+. There exists a function *f* from a set of all odd sums x^3 to a set of primes-summands *y*, or

$$f(x^3) = y$$

which is easy to compute , but hard to invert $f^{-1}(y) = ?\, x^3$.

Computational Awearing .

Function	**Cubic Group C^3**
$f(2^3) = f(3+5) = f(8) = 2$	**Rank 2 Group** 2 members,their sum is 8, 2 primes (3,5)
$f(3^3) = f(7+9+11) = f(27) = 2$	**Rank 3 Group** 3 members, their sum is 27, 2 primes (7,11)
$f(4^3) = f(13+15+17+19) =$ $= f(64) = 3$	**Rank 4 Group** 4 members, their sum is 64, 3 primes (13,17,19)
$f(5^3) = f(21+23+25+27+29) =$ $= f(125) = 2$	**Rank 5 Group** 5 members, their sum is 125, 2 primes (23, 29)
$f(6^3) = f(31+33+35+37+39+$ $41) = f(216) = 3$	**Rank 6 Group** 6 members, their sum is 216, 3 primes (31,37,41)
$f(7^3) = f(43+45+47+49+51+$ $+ 53+55) = f(343) = 3$	**Rank 7 Group** 7 members, their sum is 343, 3 primes (43, 47, 53)
$f(8^3) = f(57+59+61+63+65+$ $67+69+71) = f(512)$ $= 4$	**Rank 8 Group** 8 members, their sum is 512, 4 primes (59,61, 67,71).
$f(9^3) = f(73+75+77+79+81+$ $83+85+87+89) =$ $= f(729) = 4$	**Rank 9 Group** 9 members, their sum is 729,4 primes (73,79, 83,89).

$f(10^3) = f(91 + 93 + 95 + 97 + 99 + 101 + 103 + 105 + 107 + 109) = f(1000) = 4$

Rank 10 Group

10 members, their sum is 1000,4 primes (97,101, 107,109).

$f(11^3) = f(111 + 113 + 115 + 117 + 119 + 121 + 123 + 125 + 127 + 129 + 131) = f(1331\ 0 = 3$

Rank 11 Group

11 members , their sum is 1331,3 primes (113,127, 131)

$f(12^3) = f(133 + 135 + 137 + 139 + 141 + 143 + 145 + 147 + 149 + 151 + 153 + 155) = f(1728) = 4$

Rank 12 Group

12 members, their sum is 1728, 4 primes (137,139, 149,151)

$f(13^3) = f(157 + 159 + 161 + 163 + 165 + 167 + 169 + 171 + 173 + 175 + 177 + 179 + 181) = f(2197) = 6$

Rank 13 Group

13 members, their sum is 2197, 6 primes (157,163, 167, 173,179, 181)

$f(14^3) = f(183 + 185 + 187 + 189 + 191 + 193 + 195 + 197 + 199 + 201 + 203 + 205 + 207 + 209) = f(2744) = 4$

Rank 14 Group

14 members, their sum is 2744, 4 primes (191,193, 197,199)

$f(15^3) = f(211 + 213 + 215 + 217 + 219 + 221 + 223 + 225 + 227 + 229 + 231 + 233 + 235 + 237 + 239) = f(3375) = 6$

Rank 15 Group

15 members, their sum is 3375, 6 primes (211,223,227, 229,233,239)

$f(16^3) = f(241 + 243 + 245 + 247 + 249 + 251 + 253 + 255 + 257 + 259 + 261 + 263 + 265 + 267 + 269 + 271) = f(4096) = 6$

Rank 16 Group

16 members, their sum is 4096, 6 primes (241,251,257, 263,269,271)

$f(17^3) = f(273 + 275 + 277 + 279 + 281 + 283 + 285 + 287 + 289 + 291 + 293 + 295 + 297 + 299 + 301 + 303\ 305) = f(4913) = 4$

Rank 17 Group

17 members, their sum is 4913, 4 primes (277,281, 283,293)

$f(18^3) = f(307 + 309 + 311 + 313 + 315 + 317 + 319 + 321 + 323 + 325 + 327 + 329 + 331 + 333 + 335 + 337 + 339 + 341) = f(5832) = 6$

Rank 18 Group

18 members, their sum is 5832, 6 primes (307,311, 313,317,331,337)

$f(19^3) = f(343 + 345 + 347 + 349 +$
$351 + 353 + 355 + 357 +$
$359 + 361 + 363 + 365 +$
$367 + 369 + 371 + 373 +$
$375 + 377 + 379) =$
$f(6859) = 7$

Rank 19 Group
19 members, their sum is 6859, 7 primes (347,349, 353,359,367,373, 379)

$f(20^3) = f(381 + 383 + 385 + 387 +$
$389 + 391 + 393 + 395 +$
$397 + 399 + 401 + 403 +$
$405 + 407 + 409 + 411 +$
$413 + 415 + 417 + 419) =$
$f(8000) = 6$

Rank 20 Group
20 members, their sum is 8000, 6 primes (383,389, 397,401,409,419)

$f(21^3) = f(421 + 423 + 425 + 427 +$
$429 + 431 + 433 + 435 +$
$437 + 439 + 441 + 443 +$
$445 + 447 + 449 + 451 +$
$453 + 455 + 457 + 459 +$
$461) = f(9261) = 8$

Rank 21 Group
21 members, their sum is 9261,8 primes (421,431, 433,439,443,449,457,461)

$f(22^3) = f(463 + 465 + 467 + 469 +$
$471 + 473 + 475 + 477 +$
$479 + 481 + 483 + 485 +$
$487 + 489 + 491 + 493 +$
$495 + 497 + 499 + 501 +$
$503 + 505) = f(10648)$
$= 7$

Rank 22 Group
22 members, their sum is 10648,7 primes (483,467, 479,487,491,499,503)

$f(23^3) = f(507 + 509 + 511 + 513 +$
$515 + 517 + 519 + 521 +$
$523 + 525 + 527 + 529 +$
$531 + 533 + 535 + 537 +$
$539 + 541 + 543 + 545 +$
$547 + 549 + 551) =$
$f(12167) = 5$

Rank 23 Group
23 members, their sum is 12167,5primes (509,521, 523,541,547)

$f(24^3) = f(553 + 555 + 557 + 559 +$
$561 + 563 + 565 + 567 +$
$569 + 571 + 573 + 575 +$
$577 + 579 + 581 + 583 +$
$585 + 587 + 589 + 591 +$
$593 + 595 + 597 + 599)$
$f(13824) = 8$

Rank 24 Group
24 members, their sum is 13824,8 primes(557,563, 569,571,577,587,593,599)

$f(25^3) = f(601 + 603 + 605 + 607 +$
$609 + 611 + 613 + 615 +$
$617 + 619 + 621 + 623 +$
$625 + 627 + 629 + 631 +$
$633 + 635 + 637 + 639 +$
$641 + 643 + 645 + 647 +$
$649) = f(15625) = 8$

Rank 25 Group
25 members, their sum is 15625,8 primes(601,607, 613,617,619,631,641,647)

$f(26^3) = f(651 + 653 + 655 + 657 +$
$659 + 661 + 663 + 665 +$
$667 + 669 + 671 + 673 +$
$675 + 677 + 679 + 681 +$
$683 + 685 + 687 + 689 +$
$691 + 693 + 695 + 697 +$
$699 + 701) = f(17576)$
$= 8$

Rank 26 Group
26 members,their sum is 17576, 8 primes (653,659, 661,673,677,683,691)

$f(27^3) = f(703 + 705 + 707 + 709 +$
$711 + 713 + 715 + 717 +$
$719 + 721 + 723 + 725 +$
$727 + 729 + 731 + 733 +$
$735 + 737 + 739 + 741 +$
$743 + 745 + 747 + 749 +$
$751 + 753 + 755) =$
$f(19683) = 6$

Rank 27 Group
27 members, their sum is 119683,6 primes (,719, 727, 739,743,751)

$f(28^3) = f(757 + 759 + 761 + 763 +$
$765 + 767 + 769 + 771 +$
$773 + 775 + 777 + 779 +$
$781 + 783 + 785 + 787 +$
$789 + 791 + 793 + 795 +$
$797 + 799 + 801 + 803 +$
$805 + 807 + 809 + 811)$
$= f(21952) = 8$

Rank 28 Group
28 members, their sum is 21952,8 primes (757,761, 769,773,787,797,809,811)

$f(29^3) = f(813 + 815 + 817 + 819 +$
$821 + 823 + 825 + 827 +$
$829 + 831 + 833 + 835 +$
$837 + 839 + 841 + 843 +$
$845 + 847 + 849 + 851 +$
$853 + 855 + 857 + 859 +$
$861 + 863 + 865 + 867 +$
$869) = f(24389) = 8$

Rank 29 Group
29 members, their sum is 24389, 7 primes (,821,827, 829,853,857,859,863)

$f(30^3) = f(871 + 873 + 875 + 877 +$
$879 + 881 + 883 + 885 +$
$887 + 889 + 891 + 901 +$
$903 + 905 + 907 + 909 +$
$911 + 913 + 915 + 917 +$
$919 + 921 + 923 + 925 +$
$927 + 929 + 931 + 933 +$
$935 + 937) = f(27000)$
$= 8$

Rank 30 Group
30 members, their sum is 27000,8 primes (881,883, 887,907,911,919,929,937)

Generally,

$f(31^3) = 939 + ... + 999 = f(29791) = 9$

Rank 31 Group
31 members, 29791, 9 primes

$f(32^3) = 1001 + ... + 1063 = f(32768) = 11$

Rank 31 Group
32 members, 32768,11 primes

f (33^3) =1065 + ...+ 1129 = f (35937) = 10	**Rank 31 Group** 32, 35937,10 primes
f (34^3) =1131 + ...+ 1197 = f (39304) = 7	**Rank 34 Group** 34, 39304 ,7 primes
f (35^3) =1199 + ...+ 1267 = f (32875) = 9	**Rank 35 Group** 35, 42875,9 primes
f (36^3) =1269 + ...+ 1339 = f (46656) = 12	**Rank 36 Group** 36, 46656 ,12 primes
f (37^3) =1341 + ...+ 1413 = f (50653) = 6	**Rank 37 Group** 37, 50653 ,6 primes
f (38^3) =1415 + ...+ 1489 = f (54872) = 14	**Rank 38 Group** 38; 54872 ,14 primes
f (39^3) =1491 + ...+ 1567 = f (59319) = 10	**Rank 39 Group** 39; 59319,10 primes
f (40^3) =1569 + ...+ 1647 = f (64000) = 12	**Rank 40 Group** 40;64000,12 primes
f (41^3) =1649+ ...+ 1729 = f (68921) = 10	**Rank 41 Group** 41; 68921,10 primes
f (42^3) =1731+ ...+ 1813 = f (74088) = 11	**Rank 42 Group** 42;74088;11primes.
f (43^3) =1815+ ...+ 1899 = f (79507) = 10	**Rank 43 Group** 43;79507;10 primes
f (44^3) =1901+ ...+ 1987 = f (85184) = 10	**Rank 44 Group** 44;85184;10 primes
f (45^3) =1989+ ...+ 2077 = f (91125) = 12	**Rank 45 Group** 45;91125;12 primes
f (46^3) =2079+ ...+ 2169 = f (97336) = 14	**Rank 46 Group** 46;97336;14 primes
f (47^3) =2171+ ...+ 2263 = f (103823) = 9	**Rank 47 Group** 47;103823;9 primes
f (48^3) =22651+ ...+ 2359 = f (110592) = 15	**Rank 48 Group** 48;110592;15 primes
f (49^3) =2361+ ...+ 2457 = f (117649) = 13	**Rank 49 Group** 49;117649;13 primes
f (50^3) =2459+ ...+ 2557 = f (125000) = 12	**Rank 50 Group** 50; 125000;12 primes
f (51^3) =2559+ ...+ 2659 = f (132651) = 10	**Rank 51 Group** 51; 132651;10 primes

f (52^3) =2661+ ...+ 2763 = f (140608) = 17	**Rank 52 Group** 52; 140608;17 primes
f (53^3) =2765+ ...+ 2869 = f (148877) = 13	**Rank 53 Group** 53; 148877;13 primes
f (54^3) =2871+ ...+ 2977 = f (157464) = 13	**Rank 54 Group** 54; 157464; 13 primes
f (55^3) =2979+ ...+ 3087 = f (166375) = 12	**Rank 55 Group** 55;166375; 12 primes
f (56^3) =3089+ ...+ 3199 = f (175616) = 11	**Rank 56 Group** 56;175616; 11 primes
f (57^3) =3201+ ...+ 3313 = f (185193) = 14	**Rank 57 Group** 57;185193; 14 primes
f (58^3) =3313+ ...+ 3429 = f (195112) = 14	**Rank 58 Group** 58;195112; 14 primes
f (59^3) =3431+ ...+ 3547 = f (205379) = 17	**Rank 59 Group** 59;205379; 17 primes
f (60^3) =3549+ ...+ 3667 = f (216000) = 14	**Rank 60 Group** 60;216000;14 primes
f (61^3) =3669+ ...+ 3789 = f (226981) = 15	**Rank 61Group** 61;226981;15 primes
f (62^3) =3791+ ...+ 3913 = f (238328) = 15	**Rank 62 Group** 62; 238328; 15 primes
f (63^3) =3915+ ...+ 4039 = f (157464) = 16	**Rank 63 Group** 63; 157464; 16 primes
f (64^3) = 4041+ ...+ 4167 = f (262144) = 16	**Rank 64 Group** 64; 262144; 16 primes
f (65^3) = 4169+ ...+ 4297 = f (274625) = 17	**Rank 65 Group** 65; 274625; 17 primes
f (66^3) = 4299+ ...+ 4429 = f (287496) = 12	**Rank 66 Group** 66;287496; 12 primes
f (67^3) = 4431+ ...+ 4563 = f (300763) = 16	**Rank 67 Group** 67; 300763; 16 primes
f (68^3) = 4565+ ...+ 4699 = f (314432) = 16	**Rank 68 Group** 68; 314432; 16 primes
f (69^3) = 4701+ ...+ 4837 = f (117649) = 16	**Rank 69 Group** 69; 117649; 16 primes
f (70^3) = 4839+ ...+ 4977 = f (343000) = 16	**Rank 70 Group** 70; 343000; 16 primes

..., at last, the largest known today cubic group is

$f(6566^3) = \ldots$ + 43112357 + 43112359 + 43112361 +
+ 43112363 + 43112365 + 43112367 +
+ 43112369 + 43112371 + 43112373 +
+ 43112375 + 43112377 + 43112379 +
+ 43112381 + 43112383 + 43112385 +
+ 43112387 + 43112389 + 43112391 +
+ 43122393 + 43112395 + 43112397 +
+ 43112399 + 43122401 + 43112403 +
+ 43112405 + 43112407 + 43112409 +
+ 43112411 + 43112413 + 43112415 +
+ 43112417 + 43112419 + 43112421 +
+ 43112423 + 43112425 + 43112427 +
+ 43112429 + 43112431 + 43112433 +
+ 43112435 + 43112437 + 43112439 +
+ 43112441 + 43112443 + 43112445 +
+ 43112447 + 43112449 + 43112451 +
+ 43112453 + 43112455 + 43112457 +
+ 43112459 + 43112461 + 43112463 +
+ 43112465 + 43112467 + 43112469 +
+ 43112471 + 43112473 + 43112475 +
+ 43112477 + 43112479 + 43112481 +
+ 43112483 + 43112485 + 43112487 +
+ 43112489 + 43112491 + 43112493 +
+ 43112495 + 43112497 + 43112499 +
+ 43112501 + 43112503 + 43112505 +
+ 43112507 + 43112509 + 43112511 +
+ 43112513 + 43112515 + 43112517 +
+ 43112519 + 43112521 + 43112523 +
+ 43112525 + 43112527 + 43112529 +
+ 43112531 + 43112533 + 43112535 +
+ 43112537 + 43112539 + 43112541 +
+ 43112543 + 43112545 + 43112547 +
+ 43112549 + 43112551 + 43112553 +
+ 43112555 + 43112557 + 43112559 +
+ 43112561 + 43112563 + 43112565 +
+ 43112567 + 43112569 + 43112571 +
+ 43112573 + 43112575 + 43112577 +
+ 43112579 + 43112581 + 43112583 +
+ 43112585 + 43112587 + 43112589 +
+ 43112591 + 43112593 + 43112595 +
+ 43112597 + 43112599 + 43112601 +
+ 43112603 + 43112605 + 43112607 +
+ **43112609** + 43112611 + 43112613 +
+ 43112615 + 43112617 + 43112619 +
+ 43112621 + 43112623 + 43112625 +
+ 43112627 + 43112629 + 43112631 +
+ 43112633 + 43112635 + 43112637 +
+ 43112639 + 43112641 + 43112643 +
+ 43112645 + 43112647 + 43112649 +
+ 43112651 + 43112653 + 43112655 +
+ 43122657 + 43112659 + 43112661 +
+ 43112663 + 43112665 + 43112667 +
+ 43112669 + 43112671 + 43112673 +
+ 43112675 + 43112677 + 43112679 +
+ 43112681 + 43112683 + 43112685 +
+ 43112687 + 43112689 + 43112691 +
+ 43112693 + 43112695 + 43112697 +
+ 43112699 + 43112701 + ...

Rank 6566 Group
6566 members; their sum is $2.8307572 \cdot 10^{11}$;
tested largest prime constructed of group's members is

$2^{43112609} - 1$ [4]

Concluding remark

In comparison with prediction of Riemann zeta function by "traditional number theory" that the probability of two randomly selected integers being relatively prime is approximately equal to $6/\pi^2$, introduced owf (one way function) by some "adogmatic number theory " predicts that the probability of $n > 2$ randomly selected odd integers of given rank C^3group (r$n$$C^3$) being prime must have different meanings for different cubic groups, namely:

r2C^3 group P = 1	r12C^3 group P = 0.33	r21C^3 group P = 0.38
r3C^3 group P = 0.66	r13C^3 group P = 0.46	r22C^3 group P = 0.31
r4C^3 group P = 0.75	r14C^3 group P = 0.28	r23C^3 group P = 0.217
r5C^3 group P = 0.4	r15C^3 group P = 0.4	r24C^3 group P = 0.29
r6C^3 group P = 0.5	r16C^3 group P = 0.375	r25C^3 group P = 0.4
r7C^3 group P = 0.4	r17C^3 group P = 0.23	r26C^3 group P = 0.26
r8C^3 group P = 0.5	r18C^3 group P = 0.33	r27C^3 group P = 0.22
r9C^3 group P = 0.4	r19C^3 group P = 0.36	r28C^3 group P = 0.25
r10C^3group P =0.27	r20C^3 group P = 0.3	r29C^3 group P = 0.27

r30C^3 group P = 0.23	r36C^3 group P = 0.33	r42C^3 group P = 0.26
r31C^3 group P = 0.29	r37C^3 group P = 0.16	r43C^3 group P = 0.23
r32C^3 group P = 0.34	r38C^3 group P = 0.5	r44C^3 group P = 0.22
r33C^3 group P = 0.3	r39C^3 group P = 0.25	r45C^3 group P = 0.26
r34C^3 group P = 0.2	r40C^3 group P = 0.3	r46C^3 group P = 0.3
r35C^3 group P = 0.25	r41C^3 group P = 0.24	r47C^3 group P = 0.19

r48C^3 group P = 0.3	r54C^3 group P = 0.24	r60C^3 group P = 0.23
r49C^3 group P = 0.26	r55C^3 group P = 0.21	r61C^3 group P = 0.24
r50C^3 group P = 0.24	r56C^3 group P = 0.19	r62C^3 group P = 0.24
r51C^3 group P = 0.19	r57C^3 group P = 0.24	r63C^3 group P = 0.25
r52C^3 group P = 0.3	r58C^3 group P = 0.24	r64C^3 group P = 0.25
r53C^3 group P = 0.24	r59C^3 group P = 0.28	r65C^3 group P = 0.26, ...

where a uniform probability distribution is defined as
P(A) = number of primes of given group / total number of odd numbers of given rn C^3.

References

[1] P.K.Rashevsky. On Dogma of Natural series. *Uspechi Mathematical Sciences*,v XXVIII,4(172)243-46,1973.
[2] Obed Godreich, L.A.Levin. A hard -core predicate for any one way function. *Proc.of the 21st Ann ACM Sympos.on theory of Computing*,1989,pp 25-32.
[3] B.Zoltac. VMPC One way function and Stream Cipher. Fast Software Encryption.2004
[4] http://primes.utm.edu/largest.html

unit 7 Newtec Place Magdalen Rd
Oxford OX41RE
e-mail Michael282.eps@gmail.com