通信情報保護學會誌
第1卷, 第3號, 1991. 12

유한체에서의 이산로그 알고리즘과 구현

Discrete logarthm algorithms in finite field and their implememntations

조인호* · 임종인** · 서광석***

요 약

유한체의 이산로그 문제는 one-way 함수의 특성을 잘 나타내고 있어, 암호 시스템에 많이 응용되고 있다. 본 논문에서는 기존의 이산로그와 관련된 알고리즘들을 분석 약술하고 그중 가장 효율적인 알고리즘으로 평가되는 Coppersmith 알고리즘을 $GF(2^{127})$에서 구현한 결과를 일부분 공개한다.

1. 서 론

어떤 유한체 GF(q)의 원시원소(primitive element) g가 주어졌을때, GF(q)−{0}의 한 원소 u의 이산로그(log u:discrete logarithm)는 $1<k<q-1$, $u=g^k$를 만족하는 정수 k이다.

유한체 이론은 수학적 중요성뿐 아니라 암호학, 부호이론, 컴퓨터, 정보이론 등에 대한 폭넓은 응용때문에 주목을 받아왔다. 특히 유한체에서의 이산로그는 One-way 함수의 대표적인 예로서 여러 암호 시스템들(The Diffie-Hellman key exchange system, The Massey-Omura cryptosystem for message transmission, The Elgamal cryptosystem)에 응용되고 있다[7].

만약 효율적인 이산로그계산 알고리즘이 발견되어 진다면 이들 암호 시스템들은 불안정하게 될 것이다.

이 분야에서는 1984년 Copersmith가 발표한 알고리즘[12]이 가장 효율적인 것으로 알려져 있다. 우리는 이 알고리즘의 $GF(2^{127})$에서의 실현을 시도하였고, 그 결과로 $GF(2^{127})$에서의 이산로그 계산을 위한 database 구축에 성공하였다.

2. Coppersmith 알고리즘 이전의 방법들

여기서는 Coppersmith 알고리즘 이전의 중요한 알고리즘들인 Adleman 알고리즘과 Waterloo팀의

* 고려대학교 수학과
** 고려대학교 서창캠퍼스 수학과
*** 서남대학교 수학과

알고리즘을 분석 약술한다.

(가) Adleman의 알고리즘[1]

Adleman의 알고리즘은 큰수의 소인수 분해에 관련된 Morrison과 Brillhart의 연분수 전개방법을 이용하였다. 두정수 A, b가 주어졌을때, A가 b-smooth라는 것은 A의 모든 소인수들이 b 보다 작음을 의미한다. Adleman의 알고리즘은 유한체 GF(p)에 대한 이산로그 알고리즘이지만 Hellman과 Reyneri[5]에 의해 지적된 바 같이 $GF(2^n)$에 대해서도 적용될 수 있다. 먼저 알고리즘을 표현하기 전에 사용되어질 기호를 설명 하는 것이 필요하다. GF(2) 위에서 차수가 n인 기약다항식 p(x)를 하나 선택한다. 그러면 $GF(2^n) \simeq GF(2)[x]/p(x))$이 되는 것은 잘 알려진 사실이다[6].

[정의 2. 1]

한 다항식 $f(x) \in GF(p)[x]$, $\deg f(x) = n \geq 1$가 $GF(p^n)$의 원시원소의 GF(p) 위에서의 최소다항식일 경우 f(x)를 원시다항식(Primitive Polynomial)이라 한다.

[정리 2. 2]

n : 솟수

차수가 n인 GF(2) 위의 모든 기약 다항식들이 원시다항식이다. $\Leftrightarrow$ 2^n-1이 솟수

[정의 2. 3]

A(x)의 모든 기약인수 다항식들이 차수가 b이하일 때 A(x)는 b-smooth라고 한다. $2^{127}-1$은 솟수이므로 (정리 2. 2)에 의해서 $GF(2^{127})$을 만드는 p(x)는 원시다항식이다.

〈Adleman 알고리즘의 개요〉

1. $b = c\sqrt{n \log n}$ (c : 작은 상수)인 b를 택한다.
2. 0과 2^n-2에서 정수 m을 선택
   $x^m \equiv A(x) \bmod p(x)$라 하고
   A(x)를 Berlekamp factorization 알고리즘을 이용하여 인수분해한다[3, 6]
3. A(x)가 b-smooth인지를 test한다.
   만약 b-smooth라면
   $A(x) \equiv x^m \equiv \Pi\, q(x)^{l_q}$, $\deg q(x) \leq b$이므로,
   $m = \Sigma\, l_q \log q(x)$ in $Z/(2^n-1)$ 이다. … (*)
   만약 b-smooth가 아니면 2에서 다시 시도한다.
   Gauss 소거법을 이용하여 기약다항식들의 이산로그를 계산하여 database를 구축한다.
4. 위의 과정을 반복하여 차수가 b 이하인 기약다항식 q(x)들에 대한 이산로그 $\log q(x)$를 미지수로 하는 일차방정식 (*)들을 충분히 만든다.
5. $B(x)(\neq 0) \in GF(2^n)$의 이산로그를 찾기 위해 적당한 a를 택하여,
   $B(x) * x^a \equiv A(x) \bmod p(x)$라 하자.
   만일 $A(x) \equiv \Pi\, q(x)^{l_q}$이고
   $\deg q(x) < b$라면
   $\log B(x) \equiv e_q \Sigma \log q(x) - a \pmod{2^n-1}$.
   이므로 $\log q(x)$를 database에서 찾아 $\log B(x)$를 구할 수 있게 된다.

(나) The Waterloo 알고리즘[4].

Adleman 알고리즘의 추정 실행시간은 smoothness의 확률에 의존한다. 즉 이 알고리즘에서는 차수가 n-1 이하인 다항식인 smooth인지를 조사했다. 차수가 작은 다항식은 smooth일 확률이 크기 때문에, 만약 차수가 훨씬 작은 다항식에 대해 smooth 여부를 조사하는 방법이 있다면 더 빠른 알고리즘이 될 것이다.

Waterloo 대학의 Blake, Fuji-Hara, Mullin 그리고 Vanstone은 이러한 점에 착안하여 Adleman의 알고리즘을 개선한 새로운 알고리즘을 제시 했는데, 간단히 설명하면 다음과 같다.

database 구축에 필요했던 $A(x) \equiv x^m \bmod p(x)$에서와 실행단계인

$A(x) \equiv B(x) * x^a \bmod p(x)$에서 p(x)와 A(x)에 Extended Euclidean 알고리즘을 적용하여 그들은

$A(x) \equiv C(x)/D(x) \bmod p(x)$ ($\deg C(x) < n/2$, $\deg D(x) < n/2$)를 만족하는 다항식 $C(x)$와 $D(x)$를 얻었다.

차수가 $n-1$인 다항식이 b-smooth일 확률 보다는 차수가 $n/2$이하인 다항식이 b-smooth될 확률이 높기 때문에 이 알고리즘은 매우 효율적으로써 $GF(2^n)$에 적용시 추정시간은 $\exp(c(n\log n)^{1/2})$이다.

3. Coppersmith 알고리즘과 우리의 구현 결과

Coppersmith의 이산로그 알고리즘[12] Waterloo 알고리즘을 보다 개선한 것이다. Blake 등은 차수가 n정도인 한개 다항식의 인수분해과정을 차수가 각각 n/2정도인 두개의 다항식 인수분해과정으로 대체함으로써 Adleman의 알고리즘을 개선하였다. Coppersmith는 위 과정을 차수가 $n^{2/3}$정도인 두 다항식의 인수분해과정으로 대체함으로써 추정시간을 $\exp(c \cdot n^{1/3} \cdot (\log n)^{2/3})$의 이산로그 알고리즘을 개발하였다. 이 알고리즘은 기존의 이산로그 알고리즘 중 가장 효율적인 것으로 평가되고 있으며, 본 연구팀은 $GF(2^{127})$에 Coppersmith 알고리즘을 적용하여 15차 이하의 기약다항식 4719개에 대한 이산로그 database 구성에 성공하였다. Coppersmith 알고리즘을 먼저 기술하겠다.

차수가 n이면서 $p(x) = x^n + Q(x)$, $\deg Q(x) < n^{2/3}$인 원시다항식 $p(x)$를 선택한다.

작은 상수들 c, c'에 대해

$b \fallingdotseq c\, n^{1/3}(\log n)^{2/3}$,

$d \fallingdotseq c'\, n^{1/3}(\log n)^{2/3}$인 정수 b, d를 선택한다.

k를 $\sqrt{n/d}$에 가까운 2의 멱이라 하자.

h를 n/k 보다 큰 가장 작은 정수라 하자.

(예를 들면 : $GF(2^{127})$에서는 $p(x) = x^{127} + x + 1$, $b = 12$, $d = 10$, $k = 4$, $h = 32$으로 하였다.)

$R(x) \equiv x^{hk} \bmod p(x)$라 하면,

$R(x) = Q(x)x^{(hk-n)}$, $r = \deg R(x)$

$\gcd(A(x), B(x)) = 1$, $\deg A(x)$, $\deg B(x) < d$인

$A(x)$, $B(x)$를 선택한다.

$C(x) = A(x) * x^h + B(x)$. $D(x) \equiv C(x)^k \bmod p(x)$라 하면,

$D(x) \equiv C(x)^k \bmod p(x)$

$\equiv R(x)A(x)^k + B(x)^k \bmod p(x)$이므로,

$\deg C(x) < h + d < (nd)^{1/2}$

$\deg D(x) < h + kd < (nd)^{1/2}$이다.

$C(x) = \Pi\, q(x)^e$, $D(x) = \Pi\, q(x)^f$라 하면 ($\deg q(x) < b$)

$\Sigma(ke - f) \log q(x) \equiv$ in $Z/(2^n - 1)$이 된다.

앞의 알고리즘에서와 같은 과정을 반복함으로써 미지의 이산로그를 구하기 위한 충분한 방정식을 생성한다. 예를들면 우리는 17차 이하의 기약다항식 16510개에 대한 이산로그를 미지수로 하는 방정식 47000여개를 생성하였다.

이중 15차 이하의 것만 추출하여 앞에서와 같이 Gauss 소거법을 적용하여 database 구성에 성공하였다. database를 구성한 다음 임의의 $GF(2^n)$의 원소 $G(x)$를 여러가지 방법을 써서 차수가 많아야 b 이하인 기약다항식들로 표현한 후 database로부터 $\log G(x)$를 구한다.

부록에서 4719개의 15차 이하 기약 다항식들의 이산로그 중 일부분을 제시하였다.

부록에서 다항식이 00001F라 함은 $x^4 + x^3 + x^2 + x + 1$를 뜻한다. 프로그램은 FORTRAN으로 하였으며, IBM 3090에 구현하였다.

4. 향상된 알고리즘 및 앞으로의 전망

본 연구의 실행시 우리는 $GF(2^n)$에서의 기저로서 관용기저$\{1, x, \cdots, x^{n-1}\}$를 사용하였다. 관용기저를 사용하면 원소의 형태가 단순하게 표시되는 장점이 있지만 실행시 많은 시간을 소요하는 곱셈 및 멱승연산이 시간이 많이 걸리고 VLSI Chip 설계가 용이하지 못하다는 단점이 있다.

이러한 단점을 극복한 정규기저를 이용한 고속 연산 방법을 1982년 Massey-Omura가 제시하였고,

Itoh-Tsujii, C. C. Wang등에 의해 개선 구현 되었으며[13, 14], 특히 고속처리를 위해 승산기 설계시 EX-OR gate 수를 최소화시키는 최적 정규기저(optional normal basis)에 대해 Vanston 등[2, 11]이 연구하고 있으며, 본 연구팀도 self-dual 정규기저와 최적 정규기저와의 관계에 대해 연구하고 있으며, 내년 봄경에는 결과가 나올 것으로 예상하고 있다. 국내에서도 몇몇 학자가 이 분야에 관심을 가지고 결과를 발표하였다[16, 17].

또한 미지수 16000여개의 일차 선형 방정식을 유한체에서 풀기 위해 Gauss 소거법을 이용하였으며, 이 부분이 전 시행 과정시간의 많은 부분을 차지하였다. 이 부분은 Wiedeman의 Sparse 행렬 방법[13]을 이용하면 개선할 여지가 있다.

고속 연산이 가능한 super-computer의 등장 및 여러가지 효율적인 이산대수 계산법의 등장으로 안전성을 요하는 암호 시스템에서는 $GF(2^n)$ 적어도 $n>2000$이 되어야 된다고 생각한다[12].

참 고 문 헌

1. L. Adleman, "A subexponential for the discrete logarithm porblem with applications to cryptography," in Proc. IEEE 20th Annual Symposium on Foundations of Computer Science, 1979, pp. 55-60.

2. B. E. Agnew, R. C. Mullin, I. M. Onyszchuk and S. A. Vanstone "An Implementation for a fast Public key Cryptosystem," J of Cryptology, Vol. 3, 1991, pp. 63-79.

3. E. R. Berlekamp, "Factoring polynomials over finite fields, "Bell Syst. Tech. J., Vol. 46, pp. 1853-1859, 1967.

4. I. F. Blake, R. Fuji-Hara, R. C. Mullin, and S. A. Vanstone, "Computing logarithms in finite fields of characteistic two," to appeear in SIAM J. Algebraic and Discrete Methods.

5. M. E. Hellman and J. M. Reyneri, "Fast computation of discrete logarithms in GF(q)," Proceedings of Crypto'82, Plenum Press, 1983.

6. R. Lidle, H. Niederreiter, Finite Field, Addison-Wesley, 1983.

7. T. Itoh and S. Tsujii, "An effective recursive algorithm for computing multiplicative inverses in $GR(2^n)$," 1988 IEEE international symposium on information theory, pp. 251, june 1988.

8. D. E. Knuth, The Art of Computer Programming, Vol. 2. New York : Addison-Wesley, 1971, pp. 351-354.

9. F. J. Macwilliams and N. J. A. Slone, "The theory of Error-Correcting Codes," North-Holland, N. Y., 1977.

10. J. L. Massey and J. K. Omura, "Computational method and apparatus for finite field arithmetic, "U. S. patent, submitted 1981.

11. R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone and R. M. Wilson, "Optional normal bases in $GR(p^m)$." Discrete applied mathematics, Vol. 22, 1989, pp. 149-161.

12. A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," to appear in Proceedings of Eucrocrypt'84.

13. C. C. Wang, "VLSI architecture for computing multiplications and inverse in $GF(2^n)$," IEEE trans. on Comput., C-34, 709-177 Aug. 1985.

14. C. C. Wang, "Exponentiation in finite fields," University of California, Los Angeles, PH. D., 1985.

15. D. Wiedemann, "Solving sparse linear equations over finite fields," manuscript in preparation.

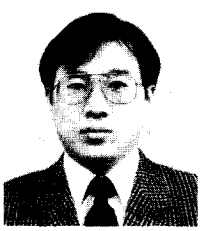
16. 이창순, 백기진, 문상래, "GF(2)상의 최적 정규기저를 갖는 기약다항식의 발견에 관한 연구" 통신정보합동학술대회 논문집, 제 1 권, 1991, pp. 36-42.

17. 조인호, 임종인, 서광석, "정규기저를 사용한 유한체에서의 고속 연산에 관한 연구," Proc. K. M. S. 1989(4).

□ 著者紹介

趙 寅 鎬(正會員)

高麗大學校 理科大學 數學科(學士)
高麗大學校 大學院 數學科(代數學 碩士)
高麗大學校 理科大學 講師/독일 뮌헨대학교 수학과(Dr. rer. nat)
서울大學校 大學院 講師/梨花女子大學校 數學科 助教授
大韓數學會 無任所 理事
大韓數學會 會誌 編輯委員/大韓數學會 監査
現 高麗大學校 理科大學 數學科 教授/韓國通信情報保護學會 副會長



임 종 인(正會員)

1980年2月 高麗大學校 數學科 卒業(學士)
1986年2月 高麗大學校 大學院 卒業(理學博士)
現 高麗大學校 自然科學大學 副教授
關心分野 : 정수론 및 관련응용분야

서 광 석 (正會員)

1982년 고대 수학과 졸업
1989년 고대 대학원 졸업(석사, 박사)
1989년 고대 부설 산업 개발 연구소 선임 연구원
1991년 서남대학 수학과

부 록

SOLUTION

INDEX	POLINOMIAL	COEFFICIENT OF POWER.
251	000937	0165674737766250931998457082560885877252
252	000938	0012717136423271261469057263253372821316
253	00093D	0166379840345691150179380712255280263497
254	000945	0036645298601856561244459908976238477384
255	000949	0084096306851653794177534762536042157272
256	000951	0055706902312003022570582143079715115711
257	000958	0107940252318750245916397428861346161216
258	000973	0054117406069505165480444177358046350418
259	000975	0013119220526682440776769841539944722955
260	00097F	0147315236074712241409037492765020477578
261	000983	0014191235666220349662894586624296363229
262	00098F	0072902248152324832234350231216864075821
263	0009AB	0161629644875347697607940740988450538511
264	0009AD	0150976547548858977485317:554534401977561
265	0009B9	0140089102183119279055693046794693224795
266	0009C7	0040474e36777821847388662963596739982747
267	0009D9	0090360374206898156463426151173319108300
268	0009E5	0094239427793279331019109939851775313717
269	0009EF	0065392121401043081556316980064631910e639
270	0009F7	0054303050954871035446546355243952159869
271	000A01	0120907857826278730026564522879 49067349
272	000A07	0118851607820464372548306728399105059174
273	000A13	0163314026707116359743077591439326000246
274	000A15	0149871978626994894146185554493948959527
275	000A29	0056170035077415451015794426220402216115
276	000A49	0128721559749434651808649569928285736963
277	000A61	0035595656145250048972277159371512132666
278	000A6D	0143018471854376941159027070091838836672
279	000A79	0011901065532825510939925343859136377784
280	000A7F	0123400566082062181479995915435469345140
281	000A85	0071703733247959870286092936597636242303
282	000A91	0014398339617546583387865260776305034913
283	000A9D	0006485062280198733003378901179248691830
284	000AA7	0055711853147075895328185324438135163893
285	000AAB	0163702656337209159293227300469098960144
286	000AB3	0068663874914224080173177559519492016231
287	000AB5	0123720298808141910538772760236512933797
288	000AD5	0108865312927895961596850242993915617646
289	000ADF	0030464251438212067509671025584279960051

290	000AE3	00395494843467149387585782044866579620l6
291	000AE9	00483811654656605170471207904301408162355
292	000AEF	00615589042609192938564369646755491309l6
293	000AF1	01178962667498947244016972[illegible]3968422
294	000AFB	00663076198225764309566796207550652291[illegible]
295	000B03	00884926550299668450186848158488419033[illegible]
296	000B09	01251345316214495252934735885158889356[illegible]
297	000B11	01387921237393828852608069463474732716[illegible]
298	000B33	01289403939427733393221411240322738432[illegible]
299	000B3F	00131204344380761717983179523903186295[illegible]
300	000B41	00448558353994685211849686005662140098[illegible]

SOLUTION

INDEX	POLINOMIAL	COEFFICIENT OF POWER.
301	000B48	01053135920318829959236695318215511805[illegible]
302	000B59	00298872751426108688615538940320338911677
303	000B5F	01521136720864342997271703261459903136[illegible]
304	000B65	00808876691804845668584496163050955963[illegible]
305	000B6F	01465357003497142945806115609929508337[illegible]
306	000B7D	00406522853582330332155460919183493698[illegible]
307	000B87	00558173717791774799806453241352686101[illegible]
308	000B8B	01099222438213873977467709887358133792[illegible]
309	000B93	00560710212776780802569424178171670312[illegible]
310	000B95	00227671158053178080072620470410903182[illegible]
311	000BAF	00261570451821990045972053351567237345[illegible]
312	000BB7	00006956974045431417225224014654108052[illegible]
313	000BBD	00166081015713558185410651020626458085[illegible]
314	000BC9	00191691882238261842196256728551990[illegible]
315	000BDB	00645043782599784591930916881471380146[illegible]
316	000BDD	00720819759204974253774029349448694085[illegible]
317	000BE7	00711457438667154478757930833679[illegible]
318	000BED	01256601512597254360169570611[illegible]
319	000C08	00456934355219084075362676574231444316[illegible]
320	000C0D	00162488533937129631965991E3[illegible]
321	000C19	01170808452864373313820877996645521412[illegible]
322	000C1F	00782712169183638727505444967480039001[illegible]
323	000C31	01460985759643610610081120500990500495[illegible]
324	000C57	00763360602130582869552370070532867605[illegible]
325	000C61	01261670668270182230126164117[illegible]
326	000C6B	01678190770857412671145377081948966982[illegible]
327	000C73	00312944079750862065553379434167971310[illegible]
328	000C75	00801075659475584081796566719210335406[illegible]
329	000C85	00348676485570134248262640200231487864[illegible]
330	000C89	00709533158891853129090712575737085908[illegible]
331	000C97	01438645268494572805642303808786719850[illegible]
332	000C98	00604785195162740440261600027223550157[illegible]
333	000C9D	00792611326506321160147587004998223690[illegible]
334	000CB3	01577986815670716525869810237057326649[illegible]
335	000CBF	01238345749995421527208341798690416240[illegible]
336	000CC7	00184663511045292[illegible]914797138518899[illegible]
337	000CCD	00411305472007612034975920820117627441[illegible]

338	000CD3	005343189210012660941987032599832174953 8
339	000CD5	008162792719398242497168748936455858167 3
340	000CE3	000979829826357341238790924731923555738 5
341	000CE9	003239115610803036335380448543373187583 4
342	000CF7	008377145113647767946435640819512354704 2
343	000D03	002301042530807737930603858400193869868 5
344	000D0F	015235728718271160000081203389167397916 2
345	000D1D	012257717568183437386277 6385938028106 0
346	000D27	008613658760167512784096270168187753326 9
347	000D2D	013894252496248276050984056308702290805 1
348	000D41	004460195689909181854007307288081568613 0
349	000D47	012057007258417991878677463424968924286 8
350	000D55	004165744430176477992441111907431595220 3

SOLUTION

INDEX	POLINOMIAL	COEFFICIENT OF POWER.
351	000D59	008483776570953224437416389586225310660 8
352	000D63	016518111955202529348095603493113668362 1
353	000D6F	007444101176599153415009245942495704718 2
354	000D71	006060548173180763984937738223742241142 5
355	000D93	016670201462140762354662703715633969686 1
356	000D9F	003065799670109610712361353166245879557 4
357	000DA9	011340402839598005929793 8106853671617 6
358	000DBB	011870499081901674485459396802651797845 7
359	000DBD	004621602354473490565133301225943724545 9
360	000DC9	000500397302088753556055733937352382080 1
361	000DD7	014445495006932751225779026263377917942 6
362	000DDB	002237818513259835285337977541066954618
363	000DE1	003310147025702996606514515634003253440 3
364	000DE7	009265218176723937753296203241774969779 6
365	000DF5	015536327579310596756371837793107057919 1
366	000DFF	008416774190051328877092909572074854848 2
367	000E05	001979824267693642558989437005162590299 3
368	000E1D	014335874877053531950540232163953862126 5
369	000E21	012956644371751864865531635462792562972 0
370	000E27	007420181615245614361539779583236600679 9
371	000E2B	016796573601566488728163181524255131771 7
372	000E33	008484308414823775532545124197320587183 4
373	000E39	012640399053053275932921877370 3.4820360
374	000E47	001894762461773581861390242039871670721
375	000E4B	001874821025809492509486697999625097323 5
376	000E55	012491388756714737235061381346538453756 5
377	000E5F	005240396917966557923840747359634459768 8
378	000E71	011260955856047664391739531542209242525 3
379	000E7B	003002539353340882699564124207000768127 4
380	000E7D	005856030367649989509169659190315883238 7
381	000E81	013651376151507015154553634162225525827
382	000E93	002423673758583057856921771362984056591 7
383	000E9F	012653976631212863566623418175909593227 3
384	000EA3	004199114534604882290320 715855190385915
385	000EBB	007847469164858078005999588578981465814 1

386	000EC9	01469653525944027510091429073088858861 98
387	000ECF	00005772756425638488490048432539329720 25
388	000EDD	00132350922895560350744664560796932700 06
389	000EF3	01464038966677737651775742039312850480 24
390	000EF9	00553374278735796086447281353147159961 44
391	000F08	00020268536536453232865800739879412117 55
392	000F19	01256868281275441327604397150461109199 84
393	000F31	00896960047557063748348686722887594592 88
394	000F37	00300458552914140209231928145455467578 62
395	000F5D	00204245916907067971692820686859237366 12
396	000F6B	00184857536127742052264673597688101800 61
397	000F6D	00395362897982687273207556091599352708 16
398	000F75	01218544129655944836864432885392083460 32
399	000F79	01091598317997883237629579951785167192 86
400	000F83	00885944201858643966636711467515611152 12

SOLUTION

INDEX	POLINOMIAL	COEFFICIENT OF POWER.
401	000F91	00508806296245138429975725393252138407 16
402	000F97	01522007759801659494119182149626817672 78
403	000F98	00052323347822590008316113940763389468 26
404	000FA7	00792885203238914463175507169649264764 23
405	000FAD	00987846828933343703224641766054151689 68
406	000FB5	01593944715131544282540356317088075176 10
407	000FCD	00781199878087570140712967058382189914 72
408	000FD3	00251763415418706735794094479888576720 387
409	000FE5	01675087300070903360619581792013134510 75
410	000FE9	01132339707169743171549417229949276358 56
411	000FFB	01498869981834900495635525978372328657 92
412	001009	00782426544974472617786057398275272362 2
413	001017	00138276084126955982101654675552024671 95
414	001021	00465289964735358937620968035433203460 05
415	001033	00207175298310567638834466975187374258 206
416	001035	01395807726059584954447348[illegible]1005
417	00103F	00821287853787830864998761255262296513 72
418	00104D	00867463900827163452839037498890954120 60
419	001053	01018409259984630775014814991746660729 63
420	001069	01228263454983466110110009391475279740 826
421	001077	00446369616707357037079917882926753511 75
422	001078	00427315820451319229309369[illegible]24783973924 4
423	00107D	00835559931565600238961413893816190345 31
424	001081	00605661487157447694102436393512419866 12
425	001088	01182556710203443861786836982533284651 71
426	001099	00804985252412011868646964340413000780 27
427	0010A3	01693498630578177274064451[illegible]56624059543 78
428	0010A5	00370256795878402069234336171769853122 29
429	0010CF	00333200165734300383622631447900462252 52
430	0010D1	00873959762528709046543493671662420759 86
431	0010EB	00913234898303340864354595[illegible]3849450008 82
432	0010ED	00604413382057111768410917537095329588 55
433	0010FF	01399192266499897023053645030651986019 60

434	001107	015782820526119171862040946800094026583 7
435	00111F	016075070088409864805370884516381211516 0
436	001123	015997899946170464626260611391228035132 8
437	001131	010187234042453688819561061636898347696
438	001137	001956692530236064762752[illegible]34108669852235
439	00113B	016706400353925106656066897313764898908 4
440	00114F	007035709080629341743464388241920856878 8
441	001157	015713301922512609884836841806417219583 9
442	001161	006027162313687660487340502365738995283 7
443	00116B	010274345176574530651300774[illegible]7469371439
444	00116D	001255778673765503268911578036257049409 0
445	001179	000468168993862912218604331659898911312 7
446	001183	012437516726978028084425404383709765988 2
447	001185	002460185822592662648037[illegible]0059599970653
448	001191	015321955084015783118928967771322547549 4
449	0011AB	015593131169521645624508839594505271184 5
450	001183	000828065172927357246891129939454149623 9

SOLUTION

INDEX	POLINOMIAL	COEFFICIENT OF POWER.
4701	00FF07	008158034805212318200831230944173737063 1
4702	00FF13	002910046814975642460723898321567150564 0
4703	00FF23	015671737313875543958427608039431514011
4704	00FF29	009858341290172985889130376041035226096 8
4705	00FF37	008182993081538546983421360165490359061 4
4706	00FF4F	010372606520534806112376582197372502824 3
4707	00FF57	016205544656767986215079728953697459476 9
4708	00FF5D	008073901306542611095648161562125040934 1
4709	00FF61	008019377432531960475973813470822969796 9
4710	00FF73	003453220449804051997612922825611734651 6
4711	00FF7F	004414265009919195223460559588434913391 9
4712	00FF8F	008848178938176081456718476227455924994 2
4713	00FF91	012969051978796642592971377033533054168 5
4714	00FFB3	012598776863795240679958562494939843542 2
4715	00FFC7	012829130530039965446291700933241299912 2
4716	00FFD9	000290448684383163333212[illegible]53642445962788 2
4717	00FFE9	012874048722074647[illegible]4793333815358713838 19
4718	00FFEF	012245209530554447668328519483744238085 8
4719	00FFFD	000000000000000018741891978888904441729