FREE"C"IZE
GUIDE TO ENTERSTELLAR LIBRARY

1. 환경구축

- 헤더파일 Enterstellar_core.h, Enterstellar_operation.h 를 추가합니다.
- 소스코드 Enterstellar_core.c, Enterstellar_operation.c , main.c 를 추가합니다.
- 변수 생성시 자료형은 bigint 로 지정해줍니다.

  예시) bigint *Big_Number = NULL;

2. 제공함수 소개

- bigint_create(변수, 워드길이) - 큰 정수 생성
- bigint_delete(동적 메모리 할당된 변수) - 큰 정수 생성 해제
- array_copy(붙여넣기할 array, 복사할 array, 워드길이) - word array 를 복사 붙여넣기
- show_bigint_hex(변수) - 16 진수로 표현하여 보여주는 함수
- show_bigint_bin(변수) - 2 진수로 표현하여 보여주는 함수
- bigint_refine(변수) - 메모리 재 할당
- bigint_gen_rand(변수, 부호, 워드길이) - 무작위의 큰 정수 생성
- array_rand(변수, 워드길이) - 무작위의 word array 생성
- bigint_assign(Y, X) - Assign bigint (Y <- X)
- CompareABS(Y, X) - 두 정수 X, Y 의 절댓값을 비교
- Compare(Y, X) - 두 정수 X, Y 의 값을 비교
- LeftShift(A, r) - r 만큼 A 를 LeftShift 시켜준다
- RightShift(A, r) - r 만큼 A 를 RightShift 시켜준다
- Reduction(A, r) - A mod 2^r 연산

- ADD(X, Y, Z) – 두 정수 X, Y 의 합을 Z 변수에 저장
- SUB(X, Y, Z) – 두 정수 X, Y 의 차를 Z 변수에 저장
- MUL(X, Y, Z) – 두 정수 X, Y 의 곱을 Z 변수에 저장
- MULC_Karatsuba(X, Y, Z) – 속도가 더 빠른 곱셈 알고리즘
- DIV(A, B, Q, R) – A 를 B 로 나누었을 때 A = B*Q + R 식을 만족하는 몫 과 나머지를 반환한다
- Sqr_Textbook(X, Y) – X^Y 연산
- Sqr_karatsuba(X, Y) - Sqr_Textbook 보다 속도가 더 빠른 X^Y 연산
- Exponentiation(X, N, Z, M) – modulo exponential

3. 계산기 기능 제공

- 큰 정수의 사칙연산이 계산기 프로그램이 제공됨(calc.c 파일 제공)
- 교육영상 - https://youtu.be/933wVlbBfqc

4. Test Vectors for Enterstellar

✧ **sign = 1** 이면 음수를 나타내고**, sign = 0** 이면 음이 아닌 정수를 나타낸다**. (8bit** 기준의 표**)**

(sign), A		(sign), B		ADD : A + B	SUB : A - B	MUL : A x B	
						NAIVE	KARATSUBA
1	0xe3b0d42eb7b00b588e4ed8	1	0x491fab1b03c15ce16447	0xe3f9f3d9d2b3ccb56fb31f	0xe367b4839cac49fbacea91	0x4109971a28c214961eae1c643a8a8033fe121c3de8	0x4109971a28c214961eae1c643a8a8033fe121c3de8
1	0x6bca67a07261c1301d2d91	0	0xdb1bae6aeced52c24369	0x6aef4bf20774d3dd5aea28	0x6ca5834edd4eae82df70fa	0x5c41ce6fc7c62b83d0c3de9009915e51c658c6a379	0x5c41ce6fc7c62b83d0c3de9009915e51c658c6a379
1	0x4d83ff93a483602f0e2454	1	0x296237ec73b182000182	0x4dad61cb90f711b10e25d6	0x4d5a9d5bb80faead0e22d2	0x0c87e165707e64964e47a063b6e27c1f8d9b52c6a8	0x0c87e165707e64964e47a063b6e27c1f8d9b52c6a8

0	0x75adf55d441206ced34a75	1	0x03a72c9f456113cdeaae	0x75aa4e30a4cca5bb055fc7	0x75b19c89e35767e2a13523	0x01ade2de44bf8d9dead788a28c395786bc045c8d86	0x01ade2de44bf8d9dead788a28c395786bc045c8d86
1	0x4790ba1fbdfc268c7e68c1	0	0xca7c5897b3376539cc63	0x46c63dc72648ef27449c5e	0x485b367855af5df1b83524	0x389af5bb5bbb5d1db53b03c9a0b9a8d6cd88554ea3	0x389af5bb5bbb5d1db53b03c9a0b9a8d6cd88554ea3
0	0xee0d25dabdb0efe57cd311	0	0x9135f3ddcad4980060ba	0xee9e5bce9b7bc47d7d33cb	0xed7befe6dfe61b4d7c7257	0x87079dee749edd8176eacb1ef56305d5c1a3d7ba5a	0x87079dee749edd8176eacb1ef56305d5c1a3d7ba5a
1	0x4cd86ac96dd3b872d0064b	0	0x05e9da4d193168c27b86	0x4cd280ef20ba870a0d8ac5	0x4cde54a3baece9db9281d1	0x01c66c969011b5b5db0e5d429fa19f7d4448bf5442	0x01c66c969011b5b5db0e5d429fa19f7d4448bf5442
0	0xaf6ff541c1f32246ce1c8d	0	0xd0b8e6a8b2f4baf1b8fd	0xb040ae286aa61701bfd58a	0xae9f3c5b19402d8bdc6390	0x8f09adcfe74e895c5d9ae00b0a64f994ef70f48f59	0x8f09adcfe74e895c5d9ae00b0a64f994ef70f48f59
1	0x70e97476d9f5e75a2df24b	1	0x1bdfe9cee85c95f22898	0x71055460a8de43f0201ae3	0x70cd948d0b0d8ac43bc9b3	0x0c4b61c4b9dd18337d75ca699503772fdd6b099488	0x0c4b61c4b9dd18337d75ca699503772fdd6b099488
0	0xa131646d6a090cdd934cb7	0	0x26b7be5c1e142407456f	0xa1581c2bc62721019a9226	0xa10aacaf0deaf8b98c0748	0x18610713b12de8b61a39708ede0a309a699b8c9659	0x18610713b12de8b61a39708ede0a309a699b8c9659

A>0		B>0		DIV: A = B x Q + R	
				Q	R
0	0xe3b0d42eb7b00b588e4ed8	0	0x491fab1b03c15ce16447	0x031d	0x093c7b9cff0d2ed91dcd
0	0x6bca67a07261c1301d2d91	0	0xdb1bae6aeced52c24369	0x7d	0xcde3763cb1dfc742434c
0	0x4d83ff93a483602f0e2454	0	0x296237ec73b182000182	0x01df	0x1538f0380a3df10b5216
0	0x75adf55d441206ced34a75	0	0x03a72c9f456113cdeaae	0x2036	0x031e0aff4d12e40e09c1

0	0x4790ba1fbdfc268c7e68c1	0	0xca7c5897b3376539cc63	0x5a	0x6102fa68faacf62c8df3
0	0xee0d25dabdb0efe57cd311	0	0x9135f3ddcad4980060ba	0x01a3	0x61d7b6bab6fb1cde82a3
0	0x4cd86ac96dd3b872d0064b	0	0x05e9da4d193168c27b86	0x0cfe	0x042893c083c9640f2f57
0	0xaf6ff541c1f32246ce1c8d	0	0xd0b8e6a8b2f4baf1b8fd	0xd7	0x24ab8a13a79945cbc012
0	0x70e97476d9f5e75a2df24b	0	0x1bdfe9cee85c95f22898	0x040c	0x1b4e45859f388a31ab2b
0	0xa131646d6a090cdd934cb7	0	0x26b7be5c1e142407456f	0x0429	0x1efd8030e742fb5371f0

X	N	M	Exponentiation 1 $x^n mod\ m$	Exponentiation 2 $nx\ mod\ m$
0xc4902b2ff9adb601909c	0x302e6442941cec8d4cae	0xfdf81f16bdc260ea5a3b	0x9798a0826b508c0bf2ae	0xf5ac12a0374732aa28d5
0x1a78c20f472261e0bfec	0xe68498f4c4f1be1df354	0xe85dc3c29d6aa0d1023a	0x554beb91c2886b925a36	0x1cfd99070ff4d8884b9a
0xfd94803e358561dce5a1	0x7d10c0b5d566ae059a44	0xbd45fcc32c2ef8a5000e	0xa0ace1728cf0a64bb3e5	0x101facd2c249f6d31e0e
0x6ca4ade278b49a91e3e1	0x71cdbfd5e68c485ecafa	0x48ba3752980c2ad9e38a	0x33ceb6d54c94b8e2692d	0x2c4e58238545c7bd5808
0x894634d83d307d319d51	0x58407b66f628e38ead87	0x41dc6e8c3843957b708a	0x3b2980302a7c3efe1bb5	0x2b5cd0e10a18d2adf5f5
0xa6e9bccd01ad61d058c1	0x40b237f706c57fbe8f14	0x3afea5c5d87b001efd8a	0x3077aa7b4ff4c8c79be3	0x36643c3aec51dd1896d8
0xdc7220ab6fc2b7e2c145	0xe389a24718c36ece842d	0xa139e21b32e51f8351db	0x7df2b49ed9c768c1bfea	0x2e6aace5447f5616019e
0x523b5d4436d9f057f517	0xb164d7b8254c0cadca67	0x76b40faa3ad2fb0233e2	0x6732c122121ad2975a9b	0x72cc99d3ae3379656b61
0x038a63a1d3090c71bda4	0xd125a1f932fd55d34c3e	0x71693b715432ea51a415	0x285f8c40827f34428324	0x507fd958bef2938ad0b8

A		SQU : A^2	
		NAIVE	KARATSUBA
1	0xe3b0d42eb7b00b588e4ed8	0xca83126f49dc2ef0bfff6846efcec015ebe00fe85640	0xca83126f49dc2ef0bfff6846efcec015ebe00fe85640
1	0x6bca67a07261c1301d2d91	0x2d62d2a7d2c4ba5cef138c20c9df86b58b0bbaf64c21	0x2d62d2a7d2c4ba5cef138c20c9df86b58b0bbaf64c21
1	0x05567089b0f2ee397b177f	0x1c7d952ee52569bc31d20fede1e2d3d7ca24321101	0x1c7d952ee52569bc31d20fede1e2d3d7ca24321101
0	0xd729fe7e845e6a6168fc1a	0xb4d7905c03dc4a1f9e06992aafc37bf497a1816332a4	0xb4d7905c03dc4a1f9e06992aafc37bf497a1816332a4
1	0xccdfa0f48501351458f7c7	0xa3f52bdf832c348238fec3fc9caeed2a2c0860a19cb1	0xa3f52bdf832c348238fec3fc9caeed2a2c0860a19cb1
0	0x8da05fee9188a1be4d7a8e	0x4e5a0e24da795b4c240de51c596c19fe1ff9bc17a6c4	0x4e5a0e24da795b4c240de51c596c19fe1ff9bc17a6c4
1	0xc91d2a68ea96088744a45f	0x9dfecfeb632b575b04199a5e8302da0f11b3ee01db41	0x9dfecfeb632b575b04199a5e8302da0f11b3ee01db41
0	0x5e73ede265f41de63a5f29	0x22d95731d953d8461ab1ee8ec45ab806a796edf37491	0x22d95731d953d8461ab1ee8ec45ab806a796edf37491
1	0x4218c15e9db1d71a32f902	0x1110c6199d1d11002d4509328d5e65156a169efce404	0x1110c6199d1d11002d4509328d5e65156a169efce404
0	0x7f958cd8f6bf3fe32923d3	0x3f95b91c86df01c63fafd10b3135e4ca77feb0995fe9	0x3f95b91c86df01c63fafd10b3135e4ca77feb0995fe9

ENTERSTELLAR LIBRARY 제작자

이름	직함
최건희	**팀장**
이용진	팀원
이현호	팀원
기윤서	인턴
김동찬	인턴