

한글 찾아보기

【 ㄱ 】	
가약성	13
가우스 정수에 의한	267
소수에 의한	44, 47
가우스, 카를 프리드리히 ..	7, 23, 89, 158, 161, 170
가우스 소수	269
곱을 나누다	280
가우스 소수 정리	272
가우스 정수	266
가약성	267, 273
공약수	282
나눗셈과 나머지	281
노름	269, 280
단원	268
단원의 노름은 1	271
소수	269, 272
소수로 유일 인수분해	279, 280
소수의 가약성	283
의 곱을 나누는 소수	280
의 기하	269, 291
의 환	269
정규화된	279
최대공약수	292
가우스 정수의 단원 정리	268
가우스 함수	172, 176
가우스의 가약성 보조정리	273, 277
가우스의 이차잉여 판정법	151, 153
가장 큰 정수 함수	176, 177
가장 특이한 소수	79
가장 홀수다운 소수	150
갈루아, 에바리스트	351
강하법	183, 229, 237, 244, 355
강한 귀납법	199
거듭제곱급수	423
거듭제곱수의 합의 생성함수	431
겔폰트, 알렉산드르 오시포비치	305
겔폰트-슈나이더 정리	305, 308
《고차 산술》	255
고차제곱수의 합 정리	437
곡선, 타원	타원곡선을 참조, 349
골드바흐 추측	89
곱셈 공식	
σ 함수	100
오일러 ϕ 함수	73, 206
곱셈완전수	104
곱셈적 함수	208
공개키 암호 체계	122, 227
공략불가 암호	119
공식	
$[a, 2a, 2a, 2a, \dots]$	410
과학적 방법	9
괴델, 쿠르트	297
굽타, 라지브	217
귀납법에 의한 증명	438
귀납법을 이용한 증명	430, 440
귀류법	102, 284, 285, 296-298, 305, 390
그랜빌, 앤드루	131
근	
원시	213, 221
근사	
디오판토스	249, 257
정리	253, 254, 258, 299, 346, 403
근사분수	
$\sqrt{2}$	397
$\sqrt{2}$	400
근사	403

기약 403
 두 칸 떨어진 403
 분자 397, 404, 419
 실수에 수렴 405
 연분수 396, 403
 인접항의 차 403
 점화식 398
 차 400, 401
 피보나치 수열 404
 근의 공식 20, 165, 411, 413
 급수
 등비급수 424
 급수, 등비 443
 기약원 292
 기하
 를 이용한 빅-오의 풀이 337
 복소수와 269, 291
 와 수론 350
 이차상호법칙의 증명 174
 기하급수적 증가
 더 빠른 357
 깊이 182
 꼬임 정리 364
 꼬임점 모임 364, 379

【 ㄴ 】
 나젤, 트뤼그베 364
 나누다 16, 27
 나누어라, 그리고 정복하라 191
 나누어진다 16, 27
 나쁜 소수 381
 네롱, 앙드레 356
 노름 269, 277, 280
 곱셈 법칙 282
 곱의 성질 270
 단원의 노름은 1 271
 노름 곱의 성질 270
 노름의 곱셈 법칙 282
 뉴욕 양키스 431
 뉴턴, 아이작 25, 62

【 ㄷ 】
 다항식
 근은 대수적이다 297
 두 개를 곱하는 시간 343
 모두 복소수 근을 가진다 266
 법 p 147
 법 p 에 대한 근 56, 59, 214
 소수 값을 가지는 202
 의 차수 343
 다항식의 곱 343
 다항식의 차수 343
 단원 268, 277
 노름 1을 가지는 271
 환 안의 276
 단위원 19, 21
 대수적 높이 355
 표준적 356
 대수적인 수 297
 대수학의 기본정리 266
 데데킨트, 리하르트 24
 데이브포트, 해럴드 255
 두 개의 제곱수로 표현 286
 두 제곱수의 합
 의 곱 184
 두 제곱수의 합 정리 193, 275, 287, 370
 소수인 경우 181, 369
 들리뉴, 피에르 383
 등비 급수 93
 등비급수 424, 443
 등비급수 공식 424
 디리실레의 디오판토스 근사 정리 403
 디리클레, 르죈 6, 23, 249, 253
 디리클레의 등차수열 정리 83
 디리클레의 디오판토스 근사 정리 .. 253, 254, 258,
 259, 299, 346
 디오판토스 근사 249, 254, 257, 365
 디오판토스 근사 정리 253, 254, 258, 259, 299, 346,
 403
 디오판토스 방정식 349
 디피, 윌필드 122

【 크 】

라그랑주, 조제프-루이스 161
 라그랑주의 네 제곱수 정리 197
 라빈-밀러 소수 판정법 132
 라빈-밀러 증인 133
 라이프니츠, 고트프리트 62
 λ (리우빌의 λ 함수) 208
 랜드리, 포춘 95
 랭런즈 프로그램 161
 레이더 217
 로그
 \log_{10} (밑이 10인 로그) 342
 \log_2 (밑이 2인 로그) 342
 n 자리수 수의 근사 342
 자연 88, 344
 지표가 닮은 226
 로피탈의 정리 443
 루츠, 엘리자베트 364
 루카스 수열 331, 430
 뤼카, 에두아르 95
 르 블랑 24
 르장드르, 아드리앵-마리 23, 89, 141, 158, 287, 298
 르장드르 기호 141, 이차상호법칙을 함께 참조,
 160, 273
 곱셈 법칙 142
 뒤집는 법 161
 의 쉬운 계산 163
 의 표 157, 159
 리베스트, 로널드 122
 리벳, 켄 24, 389
 리우빌, 조제프 298
 리우빌의 λ 함수 208
 리우빌의 부등식 300, 305
 리우빌의 수 298
 의 초월성 305
 좋은 근사에 대한 303
 리치, 존 201
 리틀우드, 존 이든저 201
 린데만, 페르디난트 298

【 코 】

마르코프 방정식 231, 331

마르코프 세 수 231, 331
 메르센, 마랭 94
 메르센 소수 93, 94, 99, 101, 103
 목록 95
 무한히 많을까? 95
 완전수와 97
 메이저, 배리 364
 모델, 루이스 조엘 354
 모델의 정리 354
 모듈라 24
 모듈라 규칙성 383, 385
 모듈라 정리 386
 모듈라 추측 24, 386
 무르티, 람 217
 무리수 265, 대수적인 수, 초월수를 함께 참조, 297
 무리수성
 $\sqrt{2}$ 의 295
 \sqrt{N} 의 305
 n 제곱근의 306
 \sqrt{p} 의 296
 무한 소수 정리 80
 $\mu(a, p)$ 169
 미적분학 .. 62, 84, 87, 89, 318, 331, 424, 425, 427,
 443
 을 이용한 빅-오의 풀이 337

【 바 】

바닥 함수 172, 176, 177
 바빌로니아 11
 바스카라차리아 243, 244
 반안정 24, 389
 반전 391
 배열
 순열 217, 222
 코스타스 217
 배중률 297
 법 51
 법 p 에 대한 다항식의 근의 정리 214
 법 4에 대해 1과 합동인 소수 정리 149, 200
 법 4에 대해 3과 합동인 소수 정리 200
 법 m 에 대한 거듭제곱 107, 108, 110, 119
 의 실행 시간 341

법 m 에 대한 피보나치 수열의 주기	327, 332
법 p 에 대한 거듭제곱	211
법 p 에 대한 이차방정식	137
법 p 에 대한 합동다항식 정리	59
법 p 에 대한 합동다항식의 근 정리	56, 147
베르누이, 다니엘	324
베버, 빌헬름	161
베시, 프레니클 드	62
베유, 앙드레	383, 386
베이즈	201
보스턴 레드삭스	431
보조정리	43
복소 평면	269, 291
복소곱	375
복소수(C)	16, 84, 89, 265
노름	269
모든 다항식은 근을 가진다	266
와 제곱수의 합	188
의 기하	269, 291
의 나눗셈	266
의 환	276
부분분수	427
부정방정식	
법 p 에 대한 해	367
부족수	104
브라마굽타	243
브로브당내그	416
브롱커, 윌리엄	244
비 판정법	425
비네의 공식	324, 331, 337, 427, 428, 430
비노그라도프, 이반	89
비둘기집 원리	251, 259
비선형 점화 수열	326
비율 판정법	424, 431
비율, 황금율	404
비잉여	138
비페리히, 아르투르	24
빗변	11
피타고라스 세 수	194
빠른 푸리에 변환(FFT)	343

【 스 】

사각 피라미드 수	441
사각-삼각수	7, 9, 233
정리	236
크기	239
사각수	5, 7, 233, 423, 439
생성함수	425
사각수의 합	433
사교수	105
사마사	243
사면체	439
사면체 수	439
이항계수	440
사원수	188
《산반서》	319
산술의 기본정리	46, 47, 79, 180, 280
삼각-사각수	7, 9, 233
정리	236
크기	239
삼각수	5, 7, 201, 233, 433, 439
n 의 합	440
n 개의 합	201
두 개의 합	240
이항계수	440
피보나치	330
삼차방정식의 근의 공식	351
삼차원 모양의 수	439
삼차잉여	143
상자 원리	251
상호법칙	
3차와 4차	161
이차	이차상호법칙을 참조, 157
생성함수	423
거듭제곱수의 합	431
고차제곱수	430
도함수	425
사각수의 수열	425
상수수열 1	424
세제곱수의 수열	429
수열	424
오일러 파이 함수	430
자연수열	425

지수 431

피보나치 수열 425, 426

샤미르, 아디 122

서랍 추론 251

서로소 27, 36, 64, 67, 69

선형 시간 알고리즘 342

선형 점화 수열 325

선형 합동방정식 정리 54, 225

선형방정식

 여러 해를 가진다 36

 최대공약수 33

 최대공약수와 33, 38

 합동 53

선형방정식 정리 38, 43, 53

세레스 161

세르, 장피에르 24, 389

세어 보기 73, 213

 법 5에 대해 2와 합동인 수 91

 소수 87

 제곱수 91

 짝수 87

세계곱수 5

 생성함수 429

Θ (빅-세타) 346

셀베르그, 아틀레 89

소수 5, 43, 79

$N^2 + 1$ 의 형태 8

$1 \pmod{3}$ 연습문제 165

$1 \pmod{4}$ 정리 165

$2^{2^k} + 1$ 의 형태 95

$2^p - 1$ 의 형태 94

$3 \pmod{4}$ 소수 정리 81

$a^2 + 2b^2$ 의 형태 189

$a^2 + 5b^2$ 의 형태 189

$a^2 + ab + b^2$ 의 형태 189

$a^2 + b^2$ 의 형태 181, 369

$a^2 + nb^2$ 의 형태 189

$a^n - 1$ 의 형태 93, 94

$N^2 + 1$ 의 형태 90

 가우스 정수 269

 가장 특이한 79

 가장 홀수스러운 79, 150

 곱을 나누다 44, 47, 280, 283

 곱의 약수 43

 관성의 소수 272

 나쁜 381

 두 제곱수의 합 6, 179, 181, 369

 등차수열 83

 라빈-밀러 판정법 132

 메르센 93, 94, 97, 99, 101, 103

 무한 80

 무한히 많은 6

 미해결 문제 89

 법 3에 대해 1과 합동 165

 법 4에 대해 1과 합동 81, 149, 200

 법 4에 대해 1과 합동 82

 법 4에 대해 3과 합동 81, 200

 법 4에 대해 5와 합동 84

 법 6에 대해 5와 합동 84

 법 m 에 대해 a 와 합동 83

 분지된 소수 272

 분해된 소수 272

 세쌍둥이 소수 9

 세어 보기 87

 셈 함수 (π) 200

 셈 함수 (π_1, π_3) 200

 소수 셈 함수 (π) 88

 소수값을 가지는 다항식 202

 쌍둥이 소수 8, 89

 유일 인수분해 46

 정리 88, 345

 짝수 79, 150

 큰 소수 찾기 110

 판별법 65, 111

 판정 125

 페르마 95

 피보나치 330

 환 안에서 292

 소수 정리 88, 345

 소수의 가약성 44, 47, 64

 소수의 거듭제곱

σ 함수 100

 소수의 거듭제곱 공식

 오일러 ϕ 함수 73, 206

소인수분해 13
 방법 47, 123
 《손자산경》 76
 수
 대수적인 297
 무리수 295
 소수 43, 79
 정렬성 원리를 가진 집합 308
 초월수 295, 298
 합성수 43
 수론
 과 기하 350
 실험적 9
 이론적 9
 해석적 89
 《수론 연구》 161
 수열, 코시 405
 수체의 체 123, 345
 수학의 역사 275
 수학적 귀납법
 강한 199
 완전 199
 수학적 귀납법 가정 198
 수학적 귀납법에 의한 증명 398
 수학적 귀납법을 사용한 증명 402
 수학적 귀납법을 이용한 증명 ... 46, 197–203, 215,
 283, 290, 317, 325
 역설적 202
 순열 배열 217, 222
 순열 행렬 222
 순환 연분수 408, 412
 $(r + s\sqrt{D})/t$ 의 꼴 412
 완전 410
 표기법 412
 순환 연분수 정리 412, 419
 슈나이더, 테오도어 305
 σ 함수 99, 205, 208
 $\sigma(mn)$ 100
 $\sigma(p^k)$ 100
 계산 100
 완전수 101
 시무라, 고로 25, 386

실수(\mathbb{R}) 16
 실행 시간 341
 쌍둥이 소수 8, 90
 쌍둥이 소수 추측 89
 【○】
 아다마르, 자크 89
 RSA 암호체계 119, 122
 아르키메데스 243
 아르키메데스의 소페 문제 243
 아벨 다양체 349
 아벨, 닐스 351
 $i(\sqrt{-1})$ 265
 아이젠슈타인, 페르디난트 169
 아이젠슈타인의 보조정리 172, 177
 아틴의 추측 216
 아틴, 에밀 161, 216, 383
 알고리즘
 “ $3n + 1$ ” 31
 다항식 곱 343
 선형 시간 342
 연속 제공 341
 연속제공법 110
 유클리드 28, 30
 의 실행 시간 341
 이차 시간 343
 인수분해 345
 추측 게임 345
 알렉산드리아의 디오판토스 229
 알포드, 윌리엄 로버트 131
 암호 119
 암호 체계
 RSA 122
 공개키 122, 227
 ElGamal 226, 227
 암호, 공략불가 119
 야코비, 카를 224
 야코비 기호 163
 약수 27
 ϕ 값의 합 205
 최대공약수 27, 282
 합 99, 100

약수 합 함수..... σ 함수를 참조, 99	연분수 점화식..... 398, 403
《어느 수학자의 변명》..... 56	연속 제공
에르되시, 폴..... 89	실행시간..... 341
에르미트, 샤를..... 305, 307	연속제공법..... 107, 108, 110, 114
에이들먼, 레너드..... 24, 122	O (빅-오)..... 335
엘가말 암호 체계..... 226, 227	$O(1)$ 337, 344
$\ln(x)$ 자연로그를 참조, 88	실행 시간 기술..... 341
엘키스, 노암..... 375	의 곱셈..... 344
역수의 합..... 344	의 기하적 풀이..... 337
연립합동방정식..... 75	의 덧셈..... 344
연분수..... 255, 391	의 정의..... 336
π 396, 401, 404	o (스몰-오)..... 346
$\sqrt{2}$ 395, 396, 400, 404, 407	$o(1)$ 346
$\sqrt{3}$ 402	오각수..... 240, 439
$\sqrt{5}$ 402	Ω (빅-오메가)..... 346
$\sqrt[3]{2}$ 394, 396	ϕ 오일러 ϕ 함수를 참조, 67
$[a, b, b, b, \dots]$ 410, 420	오일러 ϕ 함수..... 67, 113, 208
$[a, b, c, b, c, \dots]$ 419	$\phi(mn)$ 72, 206
$[b, b, b, \dots]$ 410	$\phi(p^k)$ 206
π^2 402	4의 배수..... 76
e 395, 396	계산..... 72
n 번째 근사분수..... 396, 403	곱셈 공식..... 76
\sqrt{p} 408	소수 p 의..... 68
$\sqrt{2} + \sqrt{3}$ 402	소수의 거듭제곱..... 71
근사분수..... 396, 403	소수의 거듭제곱 공식..... 73
근사분수의 귀납적 정의..... 398	약수들의 합..... 205
근사분수의 분자..... 397, 404, 419	합 공식..... 207, 215
근사분수의 차..... 400	합성수..... 73
대칭..... 421	오일러 ϕ 함수의 곱셈 공식..... 76
두 칸 떨어진 근사분수의 차..... 403	오일러 ϕ 함수
수렴..... 405	생성함수..... 430
순환..... 408	오일러 공식..... 67, 68, 71, 107, 114
순환한다..... 412	오일러 판정법..... 147, 148, 154, 171, 221
순환한다., $(r + s\sqrt{D})/t$ 412	오일러, 레온하르트 23, 89, 95, 161, 183, 188, 298, 324
완전 순환..... 410	오일러 상수..... 344
인접한 근사분수의 차..... 401, 403	오일러의 등식..... 305
제곱근..... 407, 414, 416, 417	오일러의 완전수 정리..... 99
주기..... 412	와일스, 앤드루..... 6, 25, 229, 349, 389
주기 표기법..... 412	완전 귀납법..... 199
펠 방정식..... 407, 414, 416, 417	완전 순환 연분수..... 410
피보나치 수열..... 404	완전수..... 5, 97, 104
파이..... 392	

p^k 의 형태.....	104	유클리드 호제법.....	28, 30, 34, 38, 54
$q^i p^j$ 의 형태.....	104	종료.....	30
거대한.....	99	큰 수들의 예.....	28
곱.....	104	음파탐지기.....	217
목록.....	99	이바니에츠, 헨리크.....	90
σ 함수.....	101	이진 전개.....	342
오일러.....	99	이진법 전개.....	108, 110
유클리드의 공식.....	97	이집트.....	11
짝수.....	99	이차 시간 알고리즘.....	343
홀수.....	103	이차 체.....	123, 345
원.....	19, 21	이차비잉여..... 비잉여를 참조, 138	
법 p 에 대한 해.....	376	2는?.....	153
위의 유리수점.....	21	3은?.....	154
《원론》, 유클리드.....	80, 97, 295	개수.....	139
원시 피타고라스 세 수.....	12, 15, 16, 194, 230	곱셈 법칙.....	140, 142
원시근.....	211, 213	곱셈법칙.....	140, 157
2가.....	216	르장드르 기호.....	141
가장 작은.....	221	이차상호법칙... 138, 148, 153, 157, 160, 169, 177,	
수의.....	213	183, 186, 273	
이차잉여와의 관계.....	221	일반화.....	163
정리.....	213, 221	이차잉여.....	138
지표.....	223	-1은?.....	145, 148, 160
코스타스 배열에 사용된.....	218	2는?.....	145, 153, 160, 177
월드 시리즈.....	431	3은?.....	154
월리스, 존.....	244	가우스 판정법.....	151, 153, 170
웰치, 로니.....	218	개수.....	139
위수		곱셈 법칙.....	140, 142
나눔 성질.....	212, 214	곱셈법칙.....	140, 157
법 m 에 대한 2의.....	220	르장드르 기호.....	141
법 m 에 대한 a 의.....	220	원시근과.....	221
법 p 에 대한 a 의 ($e_p(a)$).....	211	이차잉여에 대한 가우스 판정법.....	170, 172
유리수(\mathbb{Q}).....	16	이항 공식.....	314, 340
유리수점		이항 정리.....	314, 340
원 위의.....	21	법 p	315
타원곡선 위의.....	350	이항계수.....	309, 440
유사 펠 방정식.....	249, 259, 262	대칭 공식.....	314
유수.....	246	덧셈 공식.....	311
유일 인수분해.....	46	를 위한 공식.....	314
가우스 정수.....	279, 280	법 n	318
안 되는 환.....	293	법 p	315
유체론.....	161	합.....	442
유클리드.....	80, 97, 295	이항정리.....	435, 436

인수분해..... 234
 가우스 정수를 이용한..... 267
 방법..... 345
 소수..... 46
 인접한 근사분수의 차 정리..... 401, 403
 일차 합동방정식 정리..... 75
 잉여
 삼차..... 143
 제곱..... 이차잉여를 참조, 138

【 ㄴ 】
 자연로그..... 88
 자연수 (N)..... 423
 생성함수..... 425
 자연수(N)..... 5, 16
 재곱근
 연분수..... 416
 재귀
 연분수의 근사분수..... 398
 재귀 수열
 고차제곱수의 합..... 436
 재귀식
 피보나치 수열..... 320
 전개, 이진법..... 108, 110
 전개, 이항..... 342
 점화 수열
 비선형..... 326
 선형..... 325
 정규화된 가우스 정수..... 279
 정렬성 원리..... 299, 308
 정리
 $\sqrt{2}$ 의 무리수성..... 295
 ϕ 함수 공식..... 73
 σ 함수 공식..... 100
 $y^2 = x^3 + x$ 위의 유리점..... 361
 가우스 소수..... 272
 가우스 소수의 가약성..... 283
 가우스 정수 공약수..... 282
 가우스 정수 나눗셈..... 281
 가우스 정수의 단원..... 268
 가우스 정수의 유일 인수분해..... 280
 거듭제곱의 합..... 338

고차제곱수의 합..... 437
 노름 곱..... 270
 대수학의 기본정리..... 266
 두 제곱수의 합..... 181, 193, 287
 디리클레의 등차수열 정리..... 83
 디오판토스 근사..... 253, 254
 라빈-밀러..... 132
 리우빌의 부등식..... 300
 리우빌의 수의 초월성..... 305
 모델의 정리..... 354
 모듈라..... 386
 무한 소수..... 80
 법 4에 대해 1과 합동인 소수..... 149, 200
 법 4에 대해 3과 합동인 소수..... 81, 200
 법 p 에 대한 이항 정리..... 315
 비네의 공식..... 324
 사각-삼각수..... 236
 산술의 기본정리..... 46
 선형 합동방정식..... 54
 선형방정식..... 38
 소수..... 88
 소수의 가약성..... 44
 순환 연분수..... 412
 연분수 점화식..... 398
 연분수와 펠 방정식..... 417
 오일러 ϕ 함수의 합..... 207
 오일러 공식..... 68
 오일러 판정법..... 147, 221
 오일러의 완전수..... 99
 원 위의 유리수점..... 21
 원시근..... 213
 위수 나눔..... 212
 유클리드 호제법..... 30
 유클리드의 완전수..... 97
 이차상호..... 160
 이차상호법칙..... 148, 153, 164, 169, 177
 이차잉여 곱셈 법칙..... 142
 이차잉여의 수..... 139
 이항 정리..... 314
 이항계수에 대한 덧셈..... 311
 인접한 근사분수의 차..... 401
 잉여 곱셈..... 140

제곱근의 연분수.....	416	세 개의 합동식.....	77
중국인의 나머지 정리.....	75	역사.....	76
지젤의 정리.....	364	증명	
지수가 4인 경우 페르마의 마지막 정리 ..	229	과 실험.....	103, 200
지표의 계산법칙.....	224	귀납법.....	430, 438, 440
차 $D_1 - D_3$	290	귀류법 56, 102, 229, 284, 285, 296-298, 305,	
코어젤트의 정리.....	130	390	
타원곡선 위의 꼬임점.....	364	수학적 귀납법... 46, 197-203, 215, 283, 290,	
타원곡선 위의 유리수점들.....	354	317, 325, 398, 402	
타원곡선 위의 정수점.....	364	증명 마침 표시 \square	44
타원곡선의 법 p 에 대한 해.....	371, 383	지젤, 카를 루트비히.....	246, 364
페르마의 마지막 정리.....	390	지젤의 정리.....	364
페르마의 소정리.....	62, 316	지구, 공전궤도의 원주.....	393
펠 방정식.....	245, 258	지수 생성함수.....	431
피타고라스 세 수.....	15	지수적 증가.....	240
피타고라스 세 수의 빗변.....	194	gcd.....	최대공약수를 참조, 27
하세의 정리.....	383	지표.....	223
정수(\mathbb{Z}).....	16	거듭제곱 법칙.....	224
신에 의해 창조된.....	265	곱셈 법칙.....	224
정수점		로그 같은.....	226
타원곡선 위의.....	350	밑.....	223
제곱, 연속.....	107, 108, 110, 114	의 표.....	224
실행 시간.....	341	합동식의 풀이.....	224
제곱근		지표 $I(a)$	지표를 참조, 223
-1의.....	137	지표의 거듭제곱 법칙.....	224
법 m	113, 119	지표의 곱셈 법칙.....	224
연분수.....	407, 414, 417	지표의 밑.....	223
처음 n 항의 합.....	344	지표의 표.....	224
제곱수.....	5, 7	진약수 순환.....	105
두 개의 합. 179, 181, 191, 193, 286, 287, 370		짝수.....	5
두 제곱수의 합.....	6	생성함수.....	429
법 p	137	세어 보기.....	87
세어 보기.....	91	완전수.....	99
피보나치.....	330	짝수의 세계.....	44
제곱수의 합.....	6, 179, 191, 335	【 ㄷ 】	
과 복소수.....	188	차레곱 ($n!$).....	63, 91
제르맹, 소피.....	24	$(p-1)! \pmod{p}$	65
조나다 스위프트.....	416	이항계수를 위한 공식.....	314
조절합.....	433	차크라발라.....	244
조합적 수.....	309	천, 징룬.....	89, 90
좋은 근사에 대한 보조정리.....	303	체비셰프.....	200
중국인의 나머지 정리.....	71, 75		

초과수 104
 초월수 298
 $2^{\sqrt{2}}$ 은 305
 e^{π} 는 305
 e 는 305, 307
 π 는 298
 리우빌의 298, 305
 최대 정수 함수 172
 최대공약수 . 27, 유클리드 호제법을 함께 참조, 28, 30
 가우스 정수 292
 선형방정식 33
 선형방정식과 33, 38
 추측 9
 $N^2 + 1$ 90
 골드바흐 89
 쌍둥이 소수 89
 아틴의 추측 216
 추측 게임 345
 친화수 104

【 크 】

카라츠마 곱 343
 카르다노의 공식 351
 카마이클 수 111, 125, 128
 무한성 131
 서로 다른 소수의 곱 129
 최소 세 개의 소수의 곱 134
 코어젤트의 판정법 130
 홀수 129
 카마이클, 로버트 128
 코스타스 배열 217
 코스타스, 존 217
 코시 수열 405
 코어젤트의 판정법 130
 코호몰로지, l -진 369
 콕스, 데이비드 189
 쿨머, 에른스트 24
 크로네커, 레오폴트 24, 265

【 트 】

타니아마, 유타카 25, 386

타비트 벤 코라, 아불 하산 105
 타원 349
 타원곡선 24, 349
 p -결함의 유계 383
 과 페르마의 마지막 정리 389
 꼬임점 모임 364, 379
 나쁜 소수 381
 덧셈 법칙 359
 두 유리점을 지나는 직선 352
 모듈라 규칙성 383, 385
 모듈라 추측 386
 반안정 389
 법 p 에 대한 해 367
 법 p 에 대해서 약 p 개의 해를 가지는 369, 383
 복소곱 375
 소인수분해 알고리즘 123, 345
 유리수 해 350
 유리해의 크기 변화 355
 유한개의 유리수점이 있는 361
 정수해 350, 364
 타원이 아니다. 349
 판별식 364
 프라이 389
 p -결함 (a_p) 369
 테이트, 존 356
 토끼 문제 319
 통약가능한 수 295

【 프 】

파르테논 325
 파스칼, 블레즈 310
 파스칼 삼각형 309, 310
 법 p 315
 행의 합 317
 파스칼의 삼각형 442
 $\pi(x), \pi_1(x), \pi_3(x)$ 소수 썸 함수를 참조, 88
 판별식 364, 389
 페르마, 피에르 드 6, 23, 62, 95, 183, 229
 페르마 소수 95
 페르마의 강하법 229, 237, 244, 355
 페르마의 마지막 정리 6, 23, 161
 와 타원곡선 389

증명의 개요 390

지수가 4인 경우 229, 349, 363

페르마의 무한강하법 183

페르마의 소정리 .. 61, 62, 107, 125, 130, 147, 211, 212, 214, 316

제곱근 146

합성수 판별법 65, 111

펠, 존 244

펠 방정식 243, 245, 257, 258, 349, 416

±1 416, 420

연분수 407, 414

연분수에 의한 해 416, 417

펠 방정식 정리 245, 258, 416

포머런스, 칼 131

푸브리, 에티엔 24

푸생, 드 라 발레 89

프라이, 게르하르트 24

프라이 곡선 389

프로베니우스의 대각합 369

p-결합

a_p 369

나쁜 소수의 경우 381, 390

모듈라 규칙성 383, 385

상·하한 383

영 368, 371, 375

유계 383

큰 경우 383

피라미드

4차원 440, 442

사각 441

수 439

피보나치, 레오나르도 319

피보나치 생성함수 공식 426

피보나치 수열 5, 202, 337, 398, 404, 423

가약성 패턴 330

마르코프 세 수 331

법 m 326, 332

법 m 에 대한 주기 327

비네의 공식 324, 331, 337, 430

삼각수 330

생성함수 425, 426

소수 330

에 대한 항등식 330

연속된 항의 비율 322

점화식 320

제곱 330

황금비 325

피사의 레오나르도 319

피타고라스 삼각수 349

피타고라스 삼각형 11

피타고라스 세 수 6, 12, 350

빗변 194

원과 19, 21

원시 12, 16, 230

정리 15, 194

피타고라스 세 수의 빗변 정리 194

피타고라스 정리 11, 265, 295

【 ㅎ 】

하디, 고드프리 해럴드 56

하세, 헬무트 383

하세 정리 383

함수, 곱셈적 208

합

$1 + 2 + \cdots + n$ 433

$1^2 + 2^2 + \cdots + n^2$ 433

$1^k + 2^k + \cdots + n^k$ 435, 441

$T_1 + T_2 + \cdots + T_n$ 440

$1 + \frac{1}{2} + \cdots + \frac{1}{n}$ 201

$1 + \frac{1}{2} + \cdots + \frac{1}{n}$ 344

$1 + 2 + \cdots + n$ 7, 49, 335

$\sqrt{1} + \sqrt{2} + \cdots + \sqrt{n}$ 344

$1 + 3 + 5 + \cdots + (2n + 1)$ 9

$1 \cdot 2 + 2 \cdot 3 + \cdots + (n - 1)n$ 201

$1^2 + 2^2 + \cdots + n^2$ 49, 197, 199, 335

$1^3 + 2^3 + \cdots + n^3$ 201

$1^k + 2^k + \cdots + n^k$ 337

$T_1 + T_2 + \cdots + T_n$ 201

거듭제곱수 441

고차 제곱수의 6, 23, 337

고차제곱수 435

두 개의 삼각수 240

두 제곱수의 286, 287, 370

사각수 433

제곱수의 6, 179, 191, 335
 합 공식, 오일러 ϕ 함수 207, 215
 합동 51
 거듭제곱 61, 67
 나눗셈 51
 모든 해 52
 법 51
 연립방정식 75
 합동방정식
 선형방정식 53
 합동식의 나눗셈 51
 합성수 5, 43
 라빈-밀러 판정법 132
 연속적인 91
 증인 127, 133
 판별법 65, 111
 판정 125
 합성수의 증인 127, 133
 해
 법 m 에 대한 114
 해석적 정수론 89

행렬
 곱셈 222
 순열 222
 허드슨 201
 허수 137, 265
 헬만, 마틴 122
 홀수 5
 생성함수 429
 홀수인 완전수 103
 환 269
 소원 292
 안의 단원 276
 유일 인수분해성이 없는 293
 의 예 276
 황금비 255, 325
 황금율 404
 홀리, 크리스토퍼 217
 히스브라운, 로저 24, 217
 힐베르트, 다비트 161
 【 기호 】
 4차원 피라미드 440, 442

영문 찾아보기

【 A 】

Abel, Niels	351
abelian variety	349
abundant number	104
Adleman, Leonard	24, 122
Alford, W.R.	131
Algebra, Fundamental Theorem of	266
algebraic number	297
algorithm	
“ $3n + 1$ ”	31
Euclidean	28, 30
factorization	345
guessing game	345
linear time	342
polynomial multiplication	343
quadratic time	343
running time of	341
successive squaring	110, 341
<i>Alice in Wonderland</i>	391
Aliquot cycle	105
amicable pair	104
analytic number theory	89
approximation	
Diophantine	249, 257
theorem	253, 254, 258, 299, 346, 403
Archimedes	243
Arithmetic, Fundamental Theorem of	46, 180
array	
Costas	217
permutation	217, 222
Artin, Emil	161, 216, 383
Artin’s conjecture	216

【 B 】

<i>Bab Ballads</i>	391
Babylonia	11
bad prime	381
base of index	223
Bays, C.	201
Bernoulli, Daniel	324
Bessy, Frénicle de	62
Bhaskaracharya	243, 244
big-Oh	335
addition of	344
definition of	336
describes running time	341
geometric proofs of	337
multiplication of	344
$O(1)$	337, 344
big-Omega (Ω)	346
big-Theta (Θ)	346
binary expansion	108, 110, 342
Binet’s formula	324, 331, 337, 427, 428, 430
binomial coefficient	309, 440
addition formula	311
formula for	314
modulo n	318
modulo p	315
sum of	442
symmetry formula	314
binomial formula	314, 340, 435, 436
Binomial Theorem	314, 340
modulo p	315
Boston Red Sox	431
box principle	251
Brahmagupta	243

- Brobdingnags 416
 Brouncker, William 244, 418
- 【 C 】**
- calculus 62, 84, 87, 89, 331, 424, 425, 427, 443
 proof of big-Oh using 337
Canon Arithmeticus 224
 Cardano's formula 351
 Carmichael number 111, 125, 128
 has at least three prime factors 134
 infinitely many 131
 is odd 129
 is product of distinct primes 129
 Korselt's criterion 130
 Carmichael, R.D. 128
 Carroll, Lewis 391
 cattle problem of Archimedes 243
 Ceres 161
 chakravala 244
 Chebychev, P.L. 200
 Chen, Jing-run 89, 90
 Chinese remainder theorem 71, 75
 for three congruences 77
 history 76
 cipher 119
 circle 19, 21
 rational points on 21
 solution modulo p 376
 class field theory 161
 class number 246
 code, unbreakable 119
 cohomology, ℓ -adic 369
 combinatorial number 309
 commensurable numbers 295
 complete induction 199
 complex multiplication 375
 complex number (\mathbb{C}) 16, 84, 89, 265
 division by 266
 every polynomial has root 266
 geometry of 269, 291
 norm 269
 ring of 276
 sums of squares and 188
 complex plane 269, 291
 composite number 5, 43
 consecutive 91
 Rabin–Miller test 132
 tests for 65, 111, 125
 witness 127, 133
 congruence 51
 all solutions of 52
 division in 51
 linear equation and 53
 modulus of 51
 powers and 61, 67
 simultaneous 75
 congruent 51
 conjecture 9
 Artin's 216
 Goldbach 89
 $N^2 + 1$ 90
 twin prime 89
 continued fraction 255, 391, 393
 convergent 396
 difference of convergents 400
 difference of successive convergents 401
 notation for 395
 notation for periodic 412
 n^{th} convergent 396
 numerator of convergent 397, 419
 of square roots 407, 414, 416, 417
 of $[a, 2a, 2a, 2a, \dots]$ 410
 of $[a, b, b, b, \dots]$ 410, 420
 of $[a, b, c, b, c, \dots]$ 419
 of $[b, b, b, \dots]$ 410
 of $\sqrt[3]{2}$ 394, 396
 of e 395, 396
 of π 396, 401
 of $\sqrt{2}$ 395, 396, 400, 407
 of \sqrt{p} 408
 Pell's equation and 407, 414, 416, 417
 period of 412
 periodic 408, 412
 periodic, $(r + s\sqrt{D})/t$ is 412

purely periodic 410
 recursion for convergents 398
 symmetric 421
 Continued Fraction Recursion Formula 398
 contradiction, proof by 56, 102, 229, 284, 285,
 296–298, 305, 390
 convergent
 difference between 400
 difference of successive 401
 gives good approximation 403
 numerator of 397, 419
 recursion formula 398
 to continued fraction 396
 to $\sqrt{2}$ 397, 400
 Costas array 217
 Costas, J.P. 217
 counting 73, 213
 even numbers 87
 numbers congruent to 2 (mod 5) 91
 prime numbers 87
 square numbers 91
 Cox, David 189
 cryptosystem
 ElGamal 226, 227
 public key 122, 227
 RSA 122
 cube number 5
 generating function 429
 cubic formula 351
 cubic residue 143
 curve, elliptic elliptic curve를 참조, 349

【 D 】
 Dedekind, Richard 24
 deficient number 104
 degree of a polynomial 343
 Deligne, Pierre 383
 depth 182
 descent 183, 229, 237, 244, 355
 Difference of Successive Convergents Theorem 401
 Diffie, Whitfield 122
 Diophantine approximation ... 249, 254, 257, 365

Diophantine approximation theorem 253, 254, 258,
 259, 299, 346, 403
 Diophantine equation 349
 solution modulo p 367
 Diophantus of Alexandria 229
 Dirichlet, Lejeune 6, 23, 249, 253
 Dirichlet's Diophantine approximation theorem
 253, 254, 258, 259, 299, 346, 403
 Dirichlet's theorem on primes in arithmetic
 progressions 83
 discriminant 364, 389
Disquisitiones arithmeticae 161
 divide 16, 27
 divide and conquer 191
 divine proportion 325
 divisibility 13
 by a Gaussian integer 267
 by a prime 44, 47
 divisible by 16, 27
 division of congruences 51
 divisor 27
 greatest common 27, 282
 sum of 99, 100
 sum of ϕ of 205

【 E 】
 earth, circumference of orbit 393
 Egypt 11
 Eisenstein, Ferdinand 169
 Eisenstein's lemma 172, 177
Elements of Euclid 80, 97, 295
 ElGamal cryptosystem 226, 227
 Elkies, Noam 375
 ellipse 349
 elliptic curve 24, 349
 addition rule 359
 bad prime 381
 bound for p -defect 383
 complex multiplication 375
 discriminant 364
 factorization algorithm 123, 345
 Fermat's Last Theorem and 389

- Frey 389
 growth of rational solutions 355
 has approximately p solutions modulo p . 369, 383
 integer solutions 350, 364
 is not an ellipse 349
 line through two rational points 352
 modularity conjecture 386
 modularity pattern 383, 385
 p -defect (a_p) 369
 rational solutions 350
 semistable 389
 solution modulo p 367
 torsion collection 364, 379
 with few rational points 361
- end-of-proof-marker \square 44
- Erdős, Paul 89
- Euclid 80, 97, 295
- Euclidean algorithm 28, 30, 34, 38, 54
 large example 28
 terminates 30
- Euler ϕ function 71
- Euler ϕ function 67, 113
 $\phi(mn)$ 73
 $\phi(p^k)$ 71, 73
 is divisible by four 76
 of p 68
 product formula for 76
- Euler's criterion 147, 148, 154, 171, 221
- Euler's formula 67, 68, 71, 107, 114
- Euler's identity 305
- Euler's perfect number theorem 99
- Euler, Leonhard 23, 89, 95, 161, 183, 188, 298, 324
- Euler ϕ function
 generating function 430
- Euler ϕ function 208
 $\phi(mn)$ 72, 206
 $\phi(p^k)$ 206
 computation of 72
 is even 76
 sum of divisors 205
 summation formula 207, 215
- Euler's constant 344
- even number 5
 counting 87
 generating function 429
 perfect 99
- Even Number World 44
- expansion, binary 108, 110, 342
- exponential generating function 431
- exponential growth 240
 faster than 357
- 【 F 】**
- factorial ($n!$) 63, 91
 formula for binomial coefficient 314
 $(p-1)! \pmod{p}$ 65
- factorization 13, 234
 into primes 46
 methods 47, 123, 345
 using Gaussian integers 267
- Fast Fourier Transform (FFT) 343
- Father William 391
- Fermat, Pierre de 6, 23, 62, 95, 183, 229
- Fermat prime 95
- Fermat's Last Theorem 6, 23, 161
 elliptic curves and 389
 for exponent four 229, 349, 363
 proof sketch 390
- Fermat's Little Theorem 61, 62, 107, 125, 130, 147, 211, 212, 214, 316
 square root of 146
 test for composite numbers 65, 111
- Fermat's method of descent 183, 229, 237, 244, 355
- Fibonacci, Leonardo 319
- Fibonacci Generating Function Formula 426
- Fibonacci sequence 5, 202, 337, 398, 423
 Binet's formula 324, 331, 337, 430
 divisibility pattern 330
 generating function 425, 426
 golden ratio 325
 identities for 330
 Markoff triple 331
 modulo m 326, 332

period modulo m 327
 prime 330
 ratio of successive terms 322
 recursive formula 320
 square 330
 triangular number 330
 floor function 172, 176, 177
 four-dimensional pyramid 440, 442
 Fouvry, Etienne 24
 fraction, continued . continued fraction을 참조, 255
 Frey, Gerhard 24, 389
 Frey curve 389
 Frobenius, trace of 369
 function, multiplicative 208
 Fundamental Theorem of Algebra 266
 Fundamental Theorem of Arithmetic ... 46, 47, 79,
 180, 280

【 G 】

Galois, Evariste 351
 Gauss, Carl Friedrich .7, 23, 89, 151, 158, 161, 170
 Gauss's criterion for quadratic residues .. 151, 153,
 170, 172
 Gaussian Divisibility Lemma 273, 277
 Gaussian integer 266
 common divisors 282
 divisibility 267, 273
 division with remainder 281
 geometry of 269, 291
 greatest common divisor 292
 norm 269, 280
 normalized 279
 prime 269, 272
 prime divides a product of 280
 prime divisibility property 283
 ring of 269
 unique factorization into primes 279, 280
 unit 268
 unit has norm 1 271
 Gaussian prime 269
 divides a product 280
 Gaussian Prime Theorem 272

Gaussian Unit Theorem 268
 gcd greatest common divisor를 참조, 27
 Gelfond, A.O. 305
 Gelfond–Schneider theorem 305, 308
 generating function 423
 derivative of 425
 exponential 431
 of a sequence 424
 of Euler phi function 430
 of Fibonacci sequence 425, 426
 of power sums 431
 of sequence of k th powers 430
 of sequence of cubes 429
 of sequence of natural numbers 425
 of sequence of ones 424
 of sequence of squares 425
 geometric series 93, 424, 443
 Geometric Series Formula 424
 geometry
 complex numbers and 269, 291
 number theory and 350
 proof of big-Oh using 337
 proof of quadratic reciprocity 174
 Germain, Sophie 24
 Gilbert, W.S. 391
 Gödel, Kurt 297
 Goldbach's Conjecture 89
 golden ratio 255, 325
 good approximation lemma 303
 Granville, Andrew 131
 greatest common divisor .. 27, Euclidean algorithm
 을 함께 참조, 28, 30
 Gaussian integer 292
 linear equation and 33, 38
 greatest integer function 172, 176, 177
 guessing game 345
 Gulliver's Travels 416
 Gupta, Rajiv 217

【 H 】

Hadamard, Jacques 89
 Hardy, G.H. 56

- Hasse, Helmut 383
 Hasse's theorem 383
 Heath-Brown, Roger 24, 217
 height 355
 canonical 356
 Hellman, Martin 122
 Hermite, Charles 305, 307
 Hilbert, David 161
 history of mathematics 275
 Hooley, Christopher 217
 Hudson, R.H. 201
 hypotenuse 11
 Pythagorean 194
- 【 I 】**
 $i(\sqrt{-1})$ 265
 imaginary number 137, 265
 index $I(a)$ indices를 참조, 223
 indices 223
 base of 223
 like logarithms 226
 power rule 224
 product rule 224
 solving congruence with 224
 tables of 224
 induction
 complete 199
 strong 199
 induction hypothesis 198
 induction proof .. 46, 197–203, 215, 283, 290, 317,
 325, 398, 402, 430, 438, 440
 paradoxical 202
 inert prime 272
 Infinitely Many Primes Theorem 80
 integer (\mathbb{Z}) 16
 made by God 265
 point on elliptic curve 350
 irrational number 265, algebraic number,
 transcendental number를 함께 참조, 297
 irrationality
 of $\sqrt{2}$ 295
 of \sqrt{N} 305
 of n^{th} roots 306
 of \sqrt{p} 296
 irreducible element 292
 Iwaniec, Henryk 90
- 【 J 】**
 Jacobi, Carl 224
 Jacobi symbol 163
- 【 K 】**
 Karatsuba multiplication 343
 Korselt's criterion 130
 Kronecker, Leopold 24, 265
 Kummer, Ernst 24
- 【 L 】**
 L'Hôpital's rule 443
 Lagrange's Four Squares Theorem 197
 Lagrange, Joseph-Louis 161
 λ (Liouville's lambda function) 208
 Landry, Fortune 95
 Langlands Program 161
 Law of quadratic reciprocity .. quadratic reciprocity
 를 참조, 138
 Law of the Excluded Middle 297
 Le Blanc, Monsieur 24
 Leech, J. 201
 Legendre, Adrien-Marie 23, 89, 141, 158, 287, 298
 Legendre symbol 141, quadratic reciprocity
 를 함께 참조, 160, 273
 how to flip 161
 multiplication rule 142
 practical computation of 163
 table of 157, 159
 Leibniz, Gottfried 62
 lemma 43
 Lenstra, Hendrik 123
 Leonardo of Pisa 319
Liber Abbaci 319
 Lindemann, F. 298
 Linear Congruence Theorem 54, 75, 225
 linear equation

congruence and 53
 greatest common divisor and 33, 38
 has many solutions 36
 Linear Equation Theorem 38, 43, 53
 linear recurrence sequence 325
 linear time algorithm 342
 Liouville, Joseph 298
 Liouville number 298
 good approximations to 303
 transcendence of 305
 Liouville's λ function 208
 Liouville's inequality 300, 305
 Littlewood, J.E. 201
 $\ln(x)$ natural logarithm을 참조, 88
 logarithm
 approximates number of digits in n 342
 indices are like 226
 \log_{10} (log base 10) 342
 \log_2 (log base 2) 342
 natural 88, 344
 Lucas sequence 331, 430
 Lucas, E. 95
 Lutz, E. 364

【 M 】
 Markoff equation 231, 331
 Markoff triple 231, 331
Mathematician's Apology, A 56
 mathematics, history of 275
 matrix
 multiplication 222
 permutation 222
 Mazur, Barry 364
 Mersenne, Marin 94
 Mersenne prime 93, 94, 99, 101, 103
 infinitely many? 95
 list of 95
 perfect numbers and 97
 modularity 24
 Modularity conjecture 24, 386
 modularity pattern 383, 385
 Modularity theorem 386

modulus 51
 Mordell, L.J. 354
 Mordell's theorem 354
 $\mu(a, p)$ 169
 multiplication formula
 Euler ϕ function 73, 206
 σ function 100
 multiplication of polynomials 343
 multiplication property of norm 270, 282
 multiplicative function 208
 Murty, M. Ram 217

【 N 】
 Nagell, T. 364
 natural logarithm 88
 natural number (\mathbb{N}) 423
 generating function 425
 natural number (\mathbb{N}) 5, 16
 Néron, André 356
 New York Yankees 431
 Newton, Sir Isaac 25, 62
 nonlinear recurrence sequence 326
 nonresidue 138
 is 2 a? 153
 is 3 a? 154
 Legendre symbol 141
 multiplication rules 140, 142, 157
 number of 139
 norm 269, 277, 280
 multiplication property 270, 282
 unit has norm 1 271
 normalized Gaussian integer 279
 NR nonresidue를 참조, 138
 number
 algebraic 297
 composite 43
 irrational 295
 prime 43, 79
 set of has well-ordering property 308
 transcendental 295, 298
 number field sieve 123, 345
 number theory

- analytic 89
 experimental 9
 geometry and 350
 theoretical 9
- 【 O 】**
 O (big-Oh) 335
 $O(1)$ 337, 344
 o (small-oh) 346
 $o(1)$ 346
 odd number 5
 generating function 429
 odd perfect number 103
 oddest prime 79, 150
 Ω (big-Omega) 346
 order
 divisibility property 212, 214
 of 2 mod m 220
 of a mod m 220
 of a mod p ($e_p(a)$) 211
- 【 P 】**
 Parthenon 325
 partial fractions 427
 Pascal, Blaise 310
 Pascal's triangle 309, 310, 442
 modulo p 315
 sum of row 317
 p -defect
 a_p 369
 bound for 383
 for bad primes 381, 390
 large values of 383
 modularity pattern 383, 385
 zero 368, 371, 375
 Pell, John 244
 Pell's equation 243, 245, 257, 258, 349, 416
 continued fractions and 407, 414
 solution by continued fractions 416, 417
 with ± 1 416, 420
 Pell's equation theorem 245, 258, 416
 Pell-like equation 249, 259, 262
 pentagonal number 240, 439
 perfect number 5, 97, 104
 Euclid's formula for 97
 Euler's theorem 99
 even 99
 huge 99
 list of 99
 odd 103
 of the form p^k 104
 of the form $q^i p^j$ 104
 product 104
 σ function and 101
 period modulo m of the Fibonacci sequence .. 327,
 332
 periodic continued fraction 408, 412
 equals $(r + s\sqrt{D})/t$ 412
 notation for 412
 purely 410
 Periodic Continued Fraction Theorem 412, 419
 permutation array 217, 222
 permutation matrix 222
 phi (ϕ) Euler ϕ function을 참조, 67
 $\pi(x), \pi_1(x), \pi_3(x)$ prime number counting
 function을 참조, 88
 π
 continued fraction of 391
 pigeonhole principle 251, 259
 Pollard, J. 123
 polynomial
 degree of 343
 every has complex root 266
 prime values of 202
 roots are algebraic numbers 297
 roots mod p 56, 59, 147, 214
 time to multiply two 343
 Polynomial Roots Mod p Theorem 56, 59, 147, 214
 Pomerance, Carl 131
 Poussin, Ch. de la Vallée 89
 power rule for indices 224
 power series 423
 power sum generating function 431
 powers modulo m 107, 108, 110, 119

running time of	341	test if not a	65, 111
powers modulo p	211	tests for	125
PPT primitive Pythagorean triple를 참조, 12		theorem	88, 345
Prime 1 (mod 3) exercise	165	triplets	9
Prime 1 (mod 4) theorem	149, 165, 200	twins	8, 89
Prime 3 (mod 4) theorem	81, 200	unique factorization into	46
prime divisibility property	44, 47, 64	unsolved problems	89
prime number	5, 43, 79	Prime Number Theorem	88, 345
bad	381	prime power formula	
congruent to 1 (mod 3)	165	Euler ϕ function	73, 206
congruent to 1 (mod 4)	81, 82, 149, 200	σ function	100
congruent to 3 (mod 4)	81, 200	primitive Pythagorean triple	12, 15, 16, 194, 230
congruent to 4 (mod 5)	84	primitive root	211, 213
congruent to 5 (mod 6)	84	2 is a	216
congruent to a (mod m)	83	indices	223
counting	87	number of	213
counting function (π)	88, 200	relation with quadratic residues	221
counting function (π_1, π_3)	200	smallest	221
divides a product	43, 44, 47, 280, 283	theorem	213, 221
even	79, 150	used to construct Costas array	218
Fermat	95	product formula for Euler ϕ function	76
Fibonacci	330	product perfect number	104
finding large	110	product rule for indices	224
Gaussian integer	269	proof	
in a ring	292	by contradiction	56, 102, 229, 284, 285,
in arithmetic progression	83	296–298, 305, 390	
infinitely many	6, 80	by induction 46, 197–203, 215, 283, 290, 317,	
Mersenne	93, 94, 97, 99, 101, 103	325, 398, 402, 430, 438, 440	
oddest	79, 150	versus experiment	103, 200
of the form $N^2 + 1$	8	public key cryptosystem	122, 227
of the form $2^{2^k} + 1$	95	purely periodic continued fraction	410
of the form $2^p - 1$	94	pyramid	
of the form $a^2 + 2b^2$	189	four-dimensional	440, 442
of the form $a^2 + 5b^2$	189	number	439
of the form $a^2 + ab + b^2$	189	number square	441
of the form $a^2 + b^2$	181, 369	Pythagorean Hypotenuse Proposition	194
of the form $a^2 + nb^2$	189	Pythagorean Theorem	11, 265, 295
of the form $a^n - 1$	93, 94	Pythagorean triangle	11
of the form $N^2 + 1$	90	Pythagorean triple	6, 12, 349, 350
polynomial taking prime values	202	circle and	19, 21
Rabin–Miller test	132	hypotenuse	194
sum of two squares	6, 179, 181, 369	primitive	12, 16, 230

- theorem 15, 194
- 【 Q 】**
- QR quadratic residue를 참조, 138
- quadratic equation modulo p 137
- quadratic formula 20, 165, 411, 413
- quadratic nonresidue nonresidue를 참조, 138
- quadratic reciprocity. 138, 148, 153, 157, 160, 169, 177, 183, 186, 273
- generalized 163
- quadratic residue 138
- Gauss's criterion 151, 153, 170
- is -1 a? 145, 148, 160
- is 2 a? 145, 153, 160, 177
- is 3 a? 154
- Legendre symbol 141
- multiplication rules 140, 142, 157
- number of 139
- primitive roots and 221
- quadratic sieve 123, 345
- quadratic time algorithm 343
- quaternion 188
- 【 R 】**
- rabbit problem 319
- Rabin–Miller test for primality 132
- Rabin–Miller witness 133
- radar 217
- ramified prime 272
- ratio test 424
- ratio, golden 255
- rational number (\mathbb{Q}) 16
- rational point
- on circle 21
- on elliptic curve 350
- real number (\mathbb{R}) 16
- reciprocal, sum of first n 344
- reciprocity
- cubic and quartic 161
- quadratic... quadratic reciprocity를 참조, 157
- recurrence sequence
- for sums of powers 436
- linear 325
- nonlinear 326
- recursion
- continued fraction convergents 398
- Fibonacci sequence 320
- reductio ad absurdum* 56, 296, 297
- relatively prime 27, 36, 64, 67, 69
- representation as sum of two squares 286
- residue
- cubic 143
- quadratic quadratic residue를 참조, 138
- Ribet, Ken 24, 389
- ring 269
- examples of 276
- lacking unique factorization 293
- prime element 292
- unit in 276
- Rivest, Ronald 122
- root
- modulo m 113, 114, 119
- primitive 213, 221
- RSA cryptosystem 119, 122
- running time 341
- 【 S 】**
- samasa 243
- Schneider, T. 305
- Schubfachsluß 251
- scientific method 9
- Selberg, Atle 89
- semistable 24, 389
- series, geometric 93, 424, 443
- Serre, Jean-Pierre 24, 389
- Shamir, Adi 122
- Shimura, Goro 25, 386
- Siegel, C.L. 246, 364
- Siegel's theorem 364
- σ function 99, 205, 208
- computation of 100
- perfect numbers and 101
- $\sigma(mn)$ 100
- $\sigma(p^k)$ 100

simultaneous congruences 75

small-oh 346

$o(1)$ 346

sociable numbers 105

sonar 217

split prime 272

square number 5, 7, 233, 423, 439

 counting 91

 Fibonacci 330

 generating function 425

 modulo p 137

 sum of two .. 6, 179, 181, 191, 193, 286, 287, 370

square pyramid number 441

square root

 continued fraction of 407, 414, 416, 417

 of -1 137

 sum of first n 344

square-triangular number 7, 9, 233

 size of 239

 theorem 236

squaring the triangle 233

squaring, successive 107, 108, 110, 114

 running time of 341

strong induction 199

successive squaring 107, 108, 110, 114

 running time of 341

sum

$1 + 2 + \cdots + n$ 433

$1^2 + 2^2 + \cdots + n^2$ 433

$1^k + 2^k + \cdots + n^k$ 435, 441

$T_1 + T_2 + \cdots + T_n$ 440

$1 + \frac{1}{2} + \cdots + \frac{1}{n}$ 201

$1 + \frac{1}{2} + \cdots + \frac{1}{n^2}$ 344

$1 + 2 + \cdots + n$ 7, 49, 335

$\sqrt{1} + \sqrt{2} + \cdots + \sqrt{n}$ 344

$1 + 3 + 5 + \cdots + (2n + 1)$ 9

$1 \cdot 2 + 2 \cdot 3 + \cdots + (n - 1)n$ 201

$1^2 + 2^2 + \cdots + n^2$ 49, 197, 199, 335

$1^3 + 2^3 + \cdots + n^3$ 201

$1^k + 2^k + \cdots + n^k$ 337

 of higher powers 6, 23, 337, 435, 441

 of squares 6, 179, 191, 335

 of two squares 286, 287, 370

 of two triangular numbers 240

$T_1 + T_2 + \cdots + T_n$ 201

sum of divisors function σ function을 참조, 99

Sum of Powers Theorem 437

sum of squares 6, 179, 191, 335, 433

 complex numbers and 188

 product of 184

Sum of Two Squares Theorem .. 193, 275, 287, 370

 for primes 181, 369

summation formula, Euler's ϕ function ... 207, 215

Sun Tzu Suan Ching 76

Swift, Jonathan 416

[T]

tables of indices 224

Taniyama, Yutaka 25, 386

Tate, John 356

telescoping sum 433

Tenniel, Sir John 391

tetrahedral number 439

 is binomial coefficient 440

tetrahedron 439

Thabit ben Korrah, Abu-I-Hasan 105

theorem

 Binet's formula 324

 binomial 314

 binomial coefficient addition 311

 binomial modulo p 315

 Chinese remainder 75

 continued fraction and Pell's equation ... 417

 continued fraction of square root 416

 continued fraction recursion 398

 difference $D_1 - D_3$ 290

 difference of successive convergents 401

 Diophantine approximation 253, 254

 Dirichlet's on primes in arithmetic progressions 83

 Euclid's perfect number 97

 Euclidean algorithm 30

 Euler phi function summation 207

- Euler's criterion 147, 221
- Euler's formula 68
- Euler's perfect number 99
- Fermat's last 390
- Fermat's last for exponent 4 229
- Fermat's little 62, 316
- fundamental of algebra 266
- fundamental of arithmetic 46
- Gaussian integer common divisor 282
- Gaussian integer division 281
- Gaussian integer prime divisibility 283
- Gaussian integer unique factorization 280
- Gaussian prime 272
- Gaussian unit 268
- Hasse's 383
- index rule 224
- infinitely many primes 80
- integer points on elliptic curve 364
- irrationality of $\sqrt{2}$ 295
- Korselt's 130
- linear congruence 54
- linear equation 38
- Liouville inequality 300
- modularity 386
- Mordell's 354
- norm multiplication 270
- number of residues 139
- order divisibility 212
- Pell's equation 245, 258
- periodic continued fraction 412
- phi function formula 73
- points mod p on elliptic curve 371, 383
- prime divisibility property 44
- prime number 88
- primes 1 (mod 4) 149, 200
- primes 3 (mod 4) 81, 200
- Pythagorean hypotenuse 194
- Pythagorean triples 15
- quadratic reciprocity 148, 153, 160, 164, 169, 177
- Rabin-Miller 132
- rational points on circle 21
- rational points on elliptic curve 354
- rational points on $y^2 = x^3 + x$ 361
- residue multiplication 140, 142
- Siegel's 364
- sigma function formula 100
- square-triangular number 236
- sum of powers 338, 437
- sum of two squares 181, 193, 287
- torsion on elliptic curve 364
- transcendence of Liouville number 305
- Θ (big-Theta) 346
- theorem
 - primitive root 213
- three-dimensional number shapes 439
- Topsy-Turvydom 391
- torsion collection 364, 379
- torsion theorem 364
- trace of Frobenius 369
- transcendental number 298
 - $2^{\sqrt{2}}$ is 305
 - e is 305, 307
 - e^π is 305
 - Liouville's 298, 305
 - π is 298
- triangle, Pythagorean 11
- triangular number 5, 7, 201, 233, 433, 439
 - Fibonacci 330
 - is binomial coefficient 440
 - sum of n 440
 - sum of n 201
 - sum of two 240
- triangular-square number 7, 9, 233
 - size of 239
 - theorem 236
- twin prime conjecture 89
- twin primes 8, 90
- 【 U 】**
 - unbreakable code 119
 - unique factorization 46
 - Gaussian integer 279, 280
 - ring without 293

- unit 268, 277
 has norm 1 271
 in a ring 276
 unit circle 19, 21
- 【 V 】**
 Vinogradov, I.M. 89
- 【 W 】**
 Wallis, J. 244
 Weber, Wilhelm 161
- Weil, André 383, 386
 Welch, L.R. 218
 well-ordering property 299, 308
 Wieferich, A. 24
 Wiles, Andrew 6, 25, 229, 349, 389
 witness for compositeness 127, 133
 World Series 431
- 【 Z 】**
 Zahlen 16