

Author Index

- Adleman, L.M., 7, 165, 173, 176
 Araki, K., 88, 106
 Atkin, A.O.L., 50, 114, 116, 118, 119,
 146, 156, 165, 173
 Birch, B.J., 98, 114
 Blake, I.F., 24
 Boneh, D., x, 6, 166
 Buchmann, J., x, 7
 Cohen, H., 102
 Cremona, J., x
 De Marrais, J., 176
 Deligne, P., 49
 Dussé, S.R., 16
 Elkies, N., 50, 114, 115, 118, 119, 139,
 146, 173
 Erdős, P., 65
 Flassenberg, R., 176, 177
 Frey, G., 82, 86, 176
 Galbraith, S., x
 Goldwasser, S., 164, 165
 Hafner, J.L., 176
 Hellman, M.E., 7, 80
 Huang, M.-D., 165, 173, 176
 Itoh, T., 22
 Joye, M., 8
 Kaliski, B.S., 16, 17
 Karatsuba, A., 20
 Kilian, J., 164, 165
 Knuth, D.E., 63
 Koblitz, N., ix, 7, 107, 171
 Koyama, K., 8
 Lenstra, H.W. Jnr, 35, 159
 Lercier, R., 118, 133–138
 Massey, J., 22
 Maurer, M., x
 Maurer, U.M., 166, 168
 McCurley, K.S., 7, 176
 Menezes, A.J., x, 2, 82, 86
 Mestre, J.-F., 102, 104
 Meyer, B., 8
 Miller, V., ix, 7
 Miyaji, A., 79, 86
 Montgomery, P.L., 15
 Morain, F., 156, 165
 Mordell, L.J., 49
 Müller, V., x, 8, 121, 131, 133, 142
 Nyberg, K., 5
 Okamoto, T., 82
 Omura, J., 22
 van Oorschot, P., 2, 96
 Paterson, K., x
 Paulus, S., 176, 177
 Pila, J., 173
 Piveteau, J.-M., 5
 Pohlig, G.C., 7, 80
 Pollard, J.M., 80, 93, 104, 176
 Quisquater, J.-J., 8
 Rabin, M., 8
 Ramanujan, S., 49
 Rubinstein, M., x
 Rück, H.-G., 82, 86, 176
 Rueppel, R.A., 5
 Satoh, T., 88, 106
 Scheafer, E., x
 Schneier, B., 2
 Schönhage, A., 20
 Schoof, R., x, 104, 109, 118, 120, 127, 165,
 173
 Semaev, I.A., 79, 88, 106
 Seroussi, G., 77

Cambridge University Press
0521653746 - Elliptic Curves in Cryptography
I. F. Blake, G. Seroussi and N. P. Smart
Index
[More information](#)

200

AUTHOR INDEX

Shanks, D., 79, 92, 102, 168
Silverman, J.H., 88
Smart, N.P., 88, 106
Solinas, J., 76
Swan, R.G., 19
Swinerton-Dyer, H.P.F., 98

Tsujii, S., 22

Vanstone, S.A., 2, 82
Vélu, J., 134
Voloch, J.F., 82

Wiener, M.J., 96
Williams, H.C., 7, 8
Wolf, S., 166, 168

Zaba, S., x

Subject Index

- addition chain, 62
 addition–subtraction chains, 63
 affine coordinates, 30, 57–58, 60–61
 anomalous curves, 79, 86, 88–91
 Atkin primes, 116, 118–122, 140–142
 authenticity, 1

 baby step/giant step algorithm, 79, 91–93, 104, 142–144, 168, 176
 Barrett reduction, 14–15
 Bernoulli number, 49
 Birch–Swinnerton-Dyer conjecture, 98
 bit-serial multipliers, 22
 BSGS, *see* baby step/giant step algorithm

 Cantor’s algorithm, 172
 certificate of primality, 163
 Chinese Remainder Theorem, 13, 80, 109, 142, 145, 159, 160
 chord–tangent process, 32
 class group, 7, 92, 150, 176
 class number, 151, 157, 173
 CM, *see* complex multiplication
 complex multiplication, 46, 149–157, 162, 165, 173
 confidentiality, 1
 Cornacchia’s algorithm, 152, 157
 CRT, *see* Chinese Remainder Theorem

 Data Encryption Standard, 3
 Dedekind’s η -function, 49, 53, 156
 DES, *see* Data Encryption Standard
 descent via isogeny, 82–83
 DHP, *see* Diffie–Hellman problem
 Diffie–Hellman key exchange, ix, 3, 6
 Diffie–Hellman problem, 3, 166–169
 digital signature, 2
 ElGamal, ix, 3
 Nyberg–Rueppel, 5
 with message recovery, 5
 Digital Signature Algorithm, ix, 4

 diophantine equation, 152, 157
 discrete logarithm problem, 2, 3, 6, 7, 79–99, 166–169
 anomalous curves, 79, 88–91
 baby step/giant step algorithm, 79, 91–93
 elliptic curve, 57, 79–99
 hyperelliptic, 176–180
 index calculus methods, 97–98
 MOV attack, 79, 82–88
 Pohlig–Hellman, 79–82
 rho, lambda and kangaroo methods, 79, 93–97
 discriminant, 114, 119, 150–152, 156, 157, 165, 179
 division polynomials, 39–42, 115, 135
 divisor, 85, 177–179
 semi-reduced, 172
 divisor class group, 85
 DLP, *see* discrete logarithm problem
 DSA, *see* Digital Signature Algorithm
 dual isogeny, 45

 ECDLP, *see* elliptic curve, discrete logarithm problem
 ECM, *see* elliptic curve, factoring method
 ECPP, *see* elliptic curve, primality proving method
 Eisenstein series, 49, 124
 ElGamal digital signature, ix, 3
 ElGamal encryption, ix, 3
 Elkies primes, 115–116, 118–140
 elliptic curve
 admissible change of variable, 31
 applications, 159–169
 checking group order, 103–104
 determining a random point, 35
 determining group order, 101–107, 109–148
 discrete logarithm problem, 7, 57, 79–99

- discriminant, 30, 124, 134
 efficient implementation, 57–76
 endomorphism ring, 45, 149
 examples, 181–189
 characteristic two, 186–189
 odd characteristic, 181–185
 factoring method, 7, 159–162
 generating with CM, 151–157
 group law, 31–34
 isomorphism, 31, 36–38, 47
 j -invariant, 31, 47, 116, 120, 121, 123, 126, 134, 149, 153
 non-singular, 30, 31, 134
 over a finite field, 34–38
 point addition, 31–34, 57–62
 point at infinity (\mathcal{O}), 30
 point doubling, *see* point addition, 32
 point multiplication, 62–76
 primality proving method, 7, 164–166
 torsion structure, 42
- elliptic function, 29
 elliptic integrals, 29
 elliptic logarithm, p -adic, 79
 endomorphism, 34, 44
 Euclidean algorithm, 13, 16, 17, 21, 24, 25
 Euclidean domain, 76
- factor base, 178
 factoring, 92
 Fermat's Last Theorem, 29
 finite field arithmetic, 11–27
 characteristic two, 19–27
 normal bases, 22–25
 palindromic polynomial, 24
 palindromic representation, 24
 polynomial bases, 19–22
 solving quadratic equations, 26
 subfield bases, 25–26
 odd characteristic, 11–19
 Barrett reduction, 14–15
 moduli of special form, 12
 Montgomery arithmetic, 15–17
 residue number system, 13–14
 solving quadratic equations, 17–19
 square roots, 17–19
- formal group, 89
 Frobenius endomorphism, 34, 73, 110, 116, 118, 121, 140, 145
 characteristic polynomial, 115, 119, 121
 Frobenius expansion, 73–76
- Frobenius map, *see* Frobenius endomorphism
 Frobenius, trace of, x , 34, 46, 73, 79, 90, 105, 140, 153
 function field, 176
 function field sieve, 176
- Galois cohomology, 82
 Galois group, 46
 Galois representation, 46
 Goldwasser–Kilian primality test, 164
 group exponentiation, 2, 62, 63
- Hafner–McCurley method, 178–180
 half-trace, 26
 Hasse's Theorem, 34, 73, 77, 102, 107
 Hensel's Lemma, 90
 Hilbert class field, 150, 152, 155–157
 Hilbert polynomial, 150, 152–155, 157, 173
 Hilbert's Theorem 90, 83
 hyperelliptic cryptosystems, 171–180
 hyperelliptic curve, 171
 arithmetic, 171–173
 Jacobian, 8, 165, 171
 J -invariant, 173
- Igusa invariants, 174
 imaginary quadratic number field, 149
 imaginary quadratic orders, 7
 index calculus methods, 97–98
 integrity, 1
 isogeny, 44, 115, 127, 134
 computing
 characteristic two, 133–138
 odd characteristic, 122–133
 degree, 44
 kernel, 121, 123, 125, 127, 128, 134
- Jacobi's formula, 49, 124
 Jacobian, 7, 171, 176
 Jacobian representation, 58
 j -invariant, *see* elliptic curve, j -invariant
- kangaroos, 176
 Koblitz curves, 101
 Kronecker congruence relation, 51
- lambda method, 80, 92, 95
 lattice, 46, 50, 127
 Laurent series, 89
 Legendre symbol, 18, 102, 120

- Massey–Omura encryption, ix, 5
 Massey–Omura multiplier, 22
 Miller–Rabin test, 162
 modular arithmetic, 11–19
 polynomial, 19–22, 24
 modular function, 47
 modular inversion, 13, 16
 polynomial, 21
 modular multiplication, 12
 polynomial, 19
 modular polynomials, 50–55, 116, 118–
 122, 145
 variants, 52
 modular reduction, 12
 polynomial, 19
 moduli of special form, 12
 Montgomery arithmetic, 15–17
 Montgomery multiplication, 17
 Montgomery reduction, 15–16
 Mordell–Weil Theorem, 98
 morphism, 44
 MOV attack, 82–88
 MOV condition, 99
 multiplication-by- m map ($[m]$), 34
- NAF, *see* non-adjacent form
 Neron–Tate height, 98
 Newton–Raphson iteration, 89
 non-adjacent form, 67
 non-repudiation, 1
 number field sieve, 7, 176
 Nyberg–Rueppel digital signature, 5
- ONB, *see* optimal normal bases
 optimal normal bases, 22–25
- p -adic numbers, 88
 palindromic polynomial, 24
 palindromic representation, 24
 Pocklington–Lehmer primality test, 162–
 165
 Pohlig–Hellman, 80–83, 91, 168, 174
 point
 addition, 31–34, 57–62
 affine coordinates, 57–58, 60–61
 cost summary, 60, 62
 projective coordinates, 59–62
 at infinity (\mathcal{O}), 30
 compression, 76–78
 counting, x , 42, 50, 52, 101–107, 109–
 148, 181
 doubling, *see* point addition, 32
 multiplication, 57, 62–76
 and exponentiation, 63
 binary method, 63
 example of costs, 72
 m -ary method, 64
 modified m -ary method, 64
 of fixed point, 73
 precomputation, 64–66, 70, 73
 relative costs, 72
 signed m -ary window, 70
 signed digit method, 67
 sliding window method, 66
 window methods, 66
 with non-adjacent form representa-
 tion, 68
 rational, 30
 polynomial multiplication, 20
 Prime Number Theorem, 107
 projective coordinates, 22, 30, 58–62
 weighted, 58
 proof of primality, 162
 down run, 163
 public key cryptography, 1
- Ramanujan τ -function, 48
 random walk, 95
 rational point, 30
 residue number system, 13–14
 rho method, 80, 92, 96
 RSA, 6, 8
- Schoof’s algorithm, 50, 109–148, 155, 165,
 173
 SEA algorithm, 116
 Shanks and Mestre algorithm, 104
 smooth number, 159
 solving quadratic equations
 characteristic two, 26
 odd characteristic, 17–19
 subfield bases, 25–26
 subfield curves, 73, 101, 104–106, 174
 supersingular curve, 37, 45, 83
- tame and wild kangaroos, 80
 Tate module, 46
 torsion group, 40
 torsion points, 40–44, 120
 group structure, 42, 121
 trace of Frobenius, *see* Frobenius, trace
 of
 twist, 37, 38, 104, 107, 109, 146

Cambridge University Press
0521653746 - Elliptic Curves in Cryptography
I. F. Blake, G. Seroussi and N. P. Smart
Index
[More information](#)

204

SUBJECT INDEX

Weber polynomials, 155–156
Weierstrass equation, 30, 123, 127
Weierstrass form, 29
Weierstrass \wp -function, 29, 47, 127
Weil pairing, 42–45, 79, 84
zeta function, 105, 174