Answers and Hints

- **Chapter 1. Prime Numbers**

  2. They are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.
  3. Emulate the proof of Proposition 1.2.5.

- **Chapter 2. The Ring of Integers Modulo n**

  2. They are 5, 13, 3, and 8.
  3. For example, $x = 22$, $y = -39$.
  4. Hint: Use the binomial theorem and prove that if $r \geq 1$, then p divides $\binom{p}{r}$.
  7. For example, $S_1 = \{0, 1, 2, 3, 4, 5, 6\}$, $S_2 = \{1, 3, 5, 7, 9, 11, 13\}$, $S_3 = \{0, 2, 4, 6, 8, 10, 12\}$, and $S_4 = \{2, 3, 5, 7, 11, 13, 29\}$. In each we find S_i by listing the first seven numbers satisfying the ith condition, then adjust the last number if necessary so that the reductions will be distinct modulo 7.
  8. An integer is divisible by 5 if and only if the last digits is 0 or 5. An integer is divisible by 9 if and only if the sum of the digits is divisible by 9. An integer is divisible by 11 if and only if the alternating sum of the digits is divisible by 11.
  9. Hint for part (a): Use the divisibility rule you found in Exercise 1.8.

10. 71

11. 8

12. As explained on page 23, we know that $\mathbf{Z}/n\mathbf{Z}$ is a ring for any n. Thus to show that $\mathbf{Z}/p\mathbf{Z}$ is a field it suffices to show that every nonzero element $\overline{a} \in \mathbf{Z}/p\mathbf{Z}$ has an inverse. Lift a to an element $a \in \mathbf{Z}$, and set $b = p$ in Proposition 2.3.1. Because p is prime, $\gcd(a, p) = 1$, so there exists x, y such that $ax+py = 1$. Reducing this equality modulo p proves that $\overline{a}$ has an inverse $x \pmod{p}$. Alternatively, one could argue just like after Definition 2.1.16 that $\overline{a}^m = 1$ for some m, so some power of $\overline{a}$ is the inverse of $\overline{a}$.

13. 302

15. Only for $n = 1, 2$. If $n > 2$, then n is either divisible by an odd prime p or 4. If $4 \mid n$, then $2^e - 2^{e-1}$ divides $\varphi(n)$ for some $e \geq 2$, so $\varphi(n)$ is even. If an odd p divides n, then the even number $p^e - p^{e-1}$ divides $\varphi(n)$ for some $e \geq 1$.

16. The map ψ is a homomorphism since both reduction maps

$$\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \quad \text{and} \quad \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$$

are homomorphisms. It is injective because if $a \in \mathbf{Z}$ is such that $\psi(a) = 0$, then $m \mid a$ and $n \mid a$, so $mn \mid a$ (since m and n are coprime), so $a \equiv 0 \pmod{mn}$. The cardinality of $\mathbf{Z}/mn\mathbf{Z}$ is mn and the cardinality of the product $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ is also mn, so ψ must be an isomorphism. The units $(\mathbf{Z}/mn\mathbf{Z})^*$ are thus in bijection with the units $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$.

For the second part of the exercise, let $g = \gcd(m, n)$ and set $a = mn/g$. Then $a \not\equiv 0 \pmod{mn}$, but $m \mid a$ and $n \mid a$, so $a \ker(\psi)$.

17. We express the question as a system of linear equations modulo various numbers, and use the Chinese remainder theorem. Let x be the number of books. The problem asserts that

$$\begin{aligned} x &\equiv 6 \pmod{7} \\ x &\equiv 2 \pmod{6} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 0 \pmod{4} \end{aligned}$$

Applying CRT to the first pair of equations, we find that $x \equiv 20 \pmod{42}$. Applying CRT to this equation and the third, we find that $x \equiv 146 \pmod{210}$. Since 146 is not divisible by 4, we add multiples of 210 to 146 until we find the first x that is divisible by 4. The first multiple works, and we find that the aspiring mathematicians have 356 math books.

18. Note that $p = 3$ works, since $11 = 3^2 + 2$ is prime. Now suppose $p \neq 3$ is any prime such that p and $p^2 + 2$ are both prime. We must have $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. Then $p^2 \equiv 1 \pmod 3$, so $p^2 + 2 \equiv 0 \pmod 3$. Since $p^2 + 2$ is prime, we must have $p^2 + 2 = 3$, so $p = 1$, a contradiction as p is assumed prime.

19. For (a) $n = 1, 2$, see solution to Exercise 2.15. For (b), yes there are many such examples. For example, $m = 2$, $n = 4$.

20. By repeated application of multiplicativity and Equation (2.2.2) on page 31, we see that if $n = \prod_i p_i^{e_i}$ is the prime factorization of n, then

$$\varphi(n) = \prod_i (p_i^{e_i} - p_i^{e_i - 1}) = \prod_i p_i^{e_i - 1} \cdot \prod_i (p_i - 1).$$

23. 1, 6, 29, 34

24. Let $g = \gcd(12n+1, 30n+2)$. Then $g \mid 30n+2-2\cdot(12n+1) = 6n$. For the same reason, g also divides $12n + 1 - 2 \cdot (6n) = 1$, so $g = 1$, as claimed.

27. There is no primitive root modulo 8, since $(\mathbf{Z}/8\mathbf{Z})^*$ has order 4, but every element of $(\mathbf{Z}/8\mathbf{Z})^*$ has order 2. Prove that if ζ is a primitive root modulo 2^n, for $n \geq 3$, then the reduction of ζ mod 8 is a primitive root, a contradiction.

28. 2 is a primitive root modulo 125.

29. Let $\prod_{i=1}^m p_i^{e_i}$ be the prime factorization of n. Slightly generalizing Exercise 16, we see that

$$(\mathbf{Z}/n\mathbf{Z})^* \cong \prod (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*.$$

Thus $(\mathbf{Z}/n\mathbf{Z})^*$ is cyclic if and only if the product $(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*$ is cyclic. If $8 \mid n$, then there is no chance $(\mathbf{Z}/n\mathbf{Z})^*$ is cyclic, so assume $8 \nmid n$. Then by Exercise 2.28, each group $(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*$ is itself cyclic. A product of cyclic groups is cyclic if and only the orders of the factors in the product are coprime (this follows from Exercise 2.16). Thus $(\mathbf{Z}/n\mathbf{Z})^*$ is cyclic if and only if the numbers $p_i(p_i - 1)$, for $i = 1, \ldots, m$ are pairwise coprime. Since $p_i - 1$ is even, there can be at most one odd prime in the factorization of n, and we see that $(\mathbf{Z}/n\mathbf{Z})^*$ is cyclic if and only if n is an odd prime power, twice an odd prime power, or $n = 4$.

• Chapter 3. Public-Key Cryptography

1. The best case is that each letter is A. Then the question is to find the largest n such that $1 + 27 + \cdots + 27^n \leq 10^{20}$. By computing

$\log_{27}(10^{20})$, we see that $27^{13} < 10^{20}$ and $27^{14} > 10^{20}$. Thus $n \leq 13$, and since $1+27+\cdots+27^{n-1} < 27^n$, and $2 \cdot 27^{13} < 10^{20}$, it follows that $n = 13$.

2. This is not secure, since it is just equivalent to a "Ceaser Cipher," that is a permutation of the letters of the alphabet, which is well-known to be easily broken using a frequency analysis.

3. If we can compute the polynomial

$$f = (x-p)(x-q)(x-r) = x^3-(p+q+r)x^2+(pq+pr+qr)x-pqr,$$

then we can factor n by finding the roots of f, for example, using Newton's method (or Cardona's formula for the roots of a cubic). Because p, q, r, are distinct odd primes, we have

$$\varphi(n) = (p-1)(q-1)(r-1) = pqr - (pq+pr+qr) + p + q + r,$$

and

$$\sigma(n) = 1 + (p+q+r) + (pq+pr+qr) + pqr.$$

Since we know n, $\varphi(n)$, and $\sigma(n)$, we know

$$\begin{aligned} \sigma(n) - 1 - n &= (p+q+r) + (pq+pr+qr), \quad \text{and} \\ \varphi(n) - n &= (p+q+r) - (pq+pr+qr). \end{aligned}$$

We can thus compute both $p+q+r$ and $pq+pr+qr$, hence deduce f and find p, q, r.

• Chapter 4. Quadratic Reciprocity

1. They are all 1, -1, 0, and 1.

3. By Proposition 4.3.4, the value of $\left(\frac{3}{p}\right)$ depends only on the reduction $\pm p \pmod{12}$. List enough primes p such that $\pm p$ reduce to $1, 5, 7, 11$ modulo 12 and verify that the asserted formula holds for each of them.

7. Since $p = 2^{13} - 1$ is prime, there are either two solutions or no solutions to $x^2 \equiv 5 \pmod{p}$, and we can decide which using quadratic reciprocity. We have

$$\left(\frac{5}{p}\right) = (-1)^{(p-1)/2\cdot(5-1)/2}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right),$$

so there are two solutions if and only if $p = 2^{13}-1$ is $\pm 1 \bmod 5$. In fact, $p \equiv 1 \pmod{5}$, so there are two solutions.

8. We have $4^{48} = 2^{96}$. By Euler's Theorem, $2^{96} = 1$, so $x = 1$.

9. For (a), take $a = 19$ and $n = 20$. We found this example using the Chinese remainder theorem applied to 4 (mod 5) and 3 (mod 4), and used that $\left(\frac{19}{20}\right) = \left(\frac{19}{5}\right) \cdot \left(\frac{19}{4}\right) = (-1)(-1) = 1$, yet 19 is not a square modulo either 5 or 4, so is certainly not a square modulo 20.
10. Hint: First reduce to the case that $6k - 1$ is prime, by using that if p and q are primes not of the form $6k - 1$, then neither is their product. If $p = 6k - 1$ divides $n^2 + n + 1$, it divides $4n^2 + 4n + 4 = (2n + 1)^2 + 3$, so -3 is a quadratic residue modulo p. Now use quadratic reciprocity to show that -3 is not a quadratic residue modulo p.

• Chapter 5. Continued Fractions

9. Suppose $n = x^2 + y^2$, with $x, y \in \mathbf{Q}$. Let d be such that $dx, dy \in \mathbf{Z}$. Then $d^2n = (dx)^2 + (dy)^2$ is a sum of two integer squares, so by Theorem 5.7.1, if $p \mid d^2n$ and $p \equiv 3 \pmod 4$, then $\mathrm{ord}_p(d^2n)$ is even. We have $\mathrm{ord}_p(d^2n)$ is even if and only if $\mathrm{ord}_p(n)$ is even, so Theorem 5.7.1 implies that n is also a sum of two squares.
11. The squares modulo 8 are $0, 1, 4$, so a sum of two squares reduces modulo 8 to one of $0, 1, 2, 4$, or 5. Four consecutive integers that are sums of squares would reduce to four consecutive integers in the set $\{0, 1, 2, 4, 5\}$, which is impossible.

• Chapter 6. Elliptic Curves

2. The second point of intersection is $(129/100, 383/1000)$.
3. The group is cyclic of order 9, generated by $(4, 2)$. The elements of $E(K)$ are

$$\{\mathcal{O}, (4,2), (3,4), (2,4), (0,4), (0,1), (2,1), (3,1), (4,3)\}.$$

4. In part (a), the pattern is that $N_p = p + 1$. For part (b), a hint is that when $p \equiv 2 \pmod 3$, the map $x \mapsto x^3$ on $(\mathbf{Z}/p\mathbf{Z})^*$ is an automorphism, so $x \mapsto x^3 + 1$ is a bijection. Now use what you learned about squares in $\mathbf{Z}/p\mathbf{Z}$ from Chapter 4.
5. For all sufficiently large real x, the equation $y^2 = x^3 + ax + b$ has a real solution y. Thus, the group $E(\mathbf{R})$ is not countable, since $\mathbf{R}$ is not countable. But any finitely generated group is countable.
6. In a course on abstract algebra, one often proves the nontrivial fact that every subgroup of a finitely generated abelian group is finitely generated. In particular, the torsion subgroup G_{tor} is

finitely generated. However, a finitely generated abelian torsion group is finite.

7. Hint: Multiply both sides of $y^2 = x^3 + ax + b$ by a power of a common denominator, and "absorb" powers into x and y.
8. Hint: see Exercise 4.6.

References

[ACD+99] K. Aardal, S. Cavallar, B. Dodson, A. Lenstra, W. Lioen, P. L. Montgomery, B. Murphy, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand, F. Morain, A. Muffett, C.&C. Putnam, and P. Zimmermann, *Factorization of a 512-bit RSA key using the Number Field Sieve*, `http://www.loria.fr/~zimmerma/records/RSA155` (1999).

[AGP94] W. R. Alford, Andrew Granville, and Carl Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722. MR 95k:11114

[AKS02] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, to appear in Annals of Math., `http://www.cse.iitk.ac.in/users/manindra/primality.ps` (2002).

[BS76] Leonard E. Baum and Melvin M. Sweet, *Continued fractions of algebraic power series in characteristic* 2, Ann. of Math. (2) **103** (1976), no. 3, 593–610. MR 53 #13127

[Bur89] D. M. Burton, *Elementary Number Theory*, second ed., W. C. Brown Publishers, Dubuque, IA, 1989. MR 90e:11001

[Cal] C. Caldwell, *The Largest Known Primes,* `http://www.utm.edu/research/primes/largest.html`.

[Cer] Certicom, *The certicom ECC challenge,* `http://www.certicom.com/index.php?action=res,ecc_challenge`.

[Cla] Clay Mathematics Institute, *Millennium prize problems,* `http://www.claymath.org/millennium_prize_problems/`.

[Coh] H. Cohn, *A short proof of the continued fraction expansion of e,* `http://research.microsoft.com/~cohn/publications.html`.

[Coh93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 94i:11105

[Con97] John H. Conway, *The Sensual (Quadratic) Form*, Carus Mathematical Monographs, vol. 26, Mathematical Association of America, Washington, DC, 1997, With the assistance of Francis Y. C. Fung. MR 98k:11035

[CP01] R. Crandall and C. Pomerance, *Prime Numbers*, Springer-Verlag, New York, 2001, A computational perspective. MR 2002a:11007

[Cre] J. E. Cremona, `mwrank` *(computer software)*, `http://www.maths.nott.ac.uk/personal/jec/ftp/progs/`.

[Cre97] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[Dav99] H. Davenport, *The Higher Arithmetic*, seventh ed., Cambridge University Press, Cambridge, 1999, An introduction to the theory of numbers, Chapter VIII by J. H. Davenport. MR 2000k:11002

[DH76] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654. MR 55 #10141

[Eul85] Leonhard Euler, *An essay on continued fractions*, Math. Systems Theory **18** (1985), no. 4, 295–328, Translated from the Latin by B. F. Wyman and M. F. Wyman. MR 87d:01011b

[FT93] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1993. MR 94d:11078

[Guy94] R. K. Guy, *Unsolved Problems in Number Theory*, second ed., Springer-Verlag, New York, 1994, Unsolved Problems in Intuitive Mathematics, I. MR 96e:11002

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hoo67] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR 34 #7445

[HW79] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979. MR 81i:10002

[IBM01] IBM, *IBM's Test-Tube Quantum Computer Makes History,* `http://www.research.ibm.com/resources/news/20011219_quantum.shtml`.

[IR90] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second ed., Springer-Verlag, New York, 1990. MR 92e:11001

[Khi63] A. Ya. Khintchine, *Continued fractions*, Translated by Peter Wynn, P. Noordhoff Ltd., Groningen, 1963. MR 28 #5038

[Knu97] Donald E. Knuth, *The Art of Computer Programming*, third ed., Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1997, Volume 1: Fundamental algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[Knu98] ———, *The Art of Computer Programming. Vol. 2*, second ed., Addison-Wesley Publishing Co., Reading, Mass., 1998, Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing. MR 83i:68003

[Kob84] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984. MR 86c:11040

[Leh14] D. N. Lehmer, *List of Primes Numbers from* 1 *to* 10,006,721, Carnegie Institution Washington, D.C. (1914).

[Lem] F. Lemmermeyer, *Proofs of the Quadratic Reciprocity Law,* `http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`.

[Len87] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673. MR 89g:11125

[LL93] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The Development of the Number Field Sieve*, Lecture Notes in Mathematics, vol. 1554, Springer-Verlag, Berlin, 1993. MR 96m:11116

[LMG+01] Vandersypen L. M., Steffen M., Breyta G., Yannoni C. S., Sherwood M. H., and Chuang I. L., *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*, Nature **414** (2001), no. 6866, 883–887.

[LT72] S. Lang and H. Trotter, *Continued fractions for some algebraic numbers*, J. Reine Angew. Math. **255** (1972), 112–134; addendum, ibid. **267** (1974), 219–220; MR **50** #2086. MR 46 #5258

[LT74] ———, *Addendum to: Continued fractions for some algebraic numbers (J. Reine Angew. Math.* **255** *(1972), 112–134)*, J. Reine Angew. Math. **267** (1974), 219–220. MR 50 #2086

[Mor93] P. Moree, *A note on Artin's conjecture*, Simon Stevin **67** (1993), no. 3-4, 255–257. MR 95e:11106

[MS08] B. Mazur and W. Stein, *What is Riemann's Hypothesis?*, 2008, In preparation.

[NZM91] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, fifth ed., John Wiley & Sons Inc., New York, 1991. MR 91i:11001

[Old70] C. D. Olds, *The Simple Continued Fraction Expression of e*, Amer. Math. Monthly **77** (1970), 968–974.

[Per57] O. Perron, *Die Lehre von den Kettenbrüchen. Dritte, verbesserte und erweiterte Aufl. Bd. II. Analytisch-funktionentheoretische Kettenbrüche*, B. G. Teubner Verlagsgesellschaft, Stuttgart, 1957. MR 19,25c

[RSA] RSA, *The New RSA Factoring Challenge,* `http://www.rsasecurity.com/rsalabs/challenges/factoring`.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), no. 2, 120–126. MR 83m:94003

[Sag08] Sage, *Free Open Source Mathematical Software (Version 3.0.4)*, 2008, `http://www.sagemath.org`.

[Sch85] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation **44** (1985), no. 170, 483–494.

[Sho97] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509. MR 98i:11108

[Sho05] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, 2005. MR MR2151586 (2006g:11003)

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR 87g:11070

[Sin99] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday, 1999.

[Slo] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`.

[ST92] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR 93g:11003

[Wal48] H. S. Wall, *Analytic Theory of Continued Fractions*, D. Van Nostrand Company, Inc., New York, N. Y., 1948. MR 10,32d

[Wei03] E. W. Weisstein, *RSA-576 Factored,* `http://mathworld.wolfram.com/news/2003-12-05/rsa/`.

[Wil00] A. J. Wiles, *The Birch and Swinnerton-Dyer Conjecture*, `http://www.claymath.org/prize_problems/birchsd.htm`.

[Zag75] D. Zagier, *The first 50 million prime numbers*, `http://modular.fas.harvard.edu/scans/papers/zagier/`.

Index

Undergraduate Texts in Mathematics *(continued from p.ii)*

Irving: Integers, Polynomials, and Rings: A Course in Algebra.
Isaac: The Pleasures of Probability. Readings in Mathematics.
James: Topological and Uniform Spaces.
Jänich: Linear Algebra.
Jänich: Topology.
Jänich: Vector Analysis.
Kemeny/Snell: Finite Markov Chains.
Kinsey: Topology of Surfaces.
Klambauer: Aspects of Calculus.
Knoebel, Laubenbacher, Lodder, Pengelley: Mathematical Masterpieces: Further Chronicles by the Explorers.
Lang: A First Course in Calculus. Fifth edition.
Lang: Calculus of Several Variables. Third edition.
Lang: Introduction to Linear Algebra. Second edition.
Lang: Linear Algebra. Third edition.
Lang: Short Calculus: The Original Edition of "A First Course in Calculus."
Lang: Undergraduate Algebra. Third edition.
Lang: Undergraduate Analysis.
Laubenbacher/Pengelley: Mathematical Expeditions.
Lax/Burstein/Lax: Calculus with Applications and Computing. Volume 1.
LeCuyer: College Mathematics with APL.
Lidl/Pilz: Applied Abstract Algebra. Second edition.
Logan: Applied Partial Differential Equations, Second edition.
Logan: A First Course in Differential Equations.
Lovász/Pelikán/Vesztergombi: Discrete Mathematics.
Macki-Strauss: Introduction to Optimal Control Theory.
Malitz: Introduction to Mathematical Logic.
Marsden/Weinstein: Calculus I, II, III. Second edition.
Martin: Counting: The Art of Enumerative Combinatorics.
Martin: The Foundations of Geometry and the Non-Euclidean Plane.
Martin: Geometric Constructions.
Martin: Transformation Geometry: An Introduction to Symmetry.
Millman/Parker: Geometry: A Metric Approach with Models. Second edition.
Moschovakis: Notes on Set Theory. Second edition.
Owen: A First Course in the Mathematical Foundations of Thermodynamics.
Palka: An Introduction to Complex Function Theory.
Pedrick: A First Course in Analysis.
Peressini/Sullivan/Uhl: The Mathematics of Nonlinear Programming.
Prenowitz/Jantosciak: Join Geometries.
Priestley: Calculus: A Liberal Art. Second edition.
Protter/Morrey: A First Course in Real Analysis. Second edition.
Protter/Morrey: Intermediate Calculus. Second edition.
Pugh: Real Mathematical Analysis.
Roman: An Introduction to Coding and Information Theory.
Roman: Introduction to the Mathematics of Finance: From Risk management to options Pricing.
Ross: Differential Equations: An Introduction with Mathematica®. Second Edition.
Ross: Elementary Analysis: The Theory of Calculus.
Samuel: Projective Geometry. *Readings in Mathematics.*
Saxe: Beginning Functional Analysis
Scharlau/Opolka: From Fermat to Minkowski.
Schiff: The Laplace Transform: Theory and Applications.
Sethuraman: Rings, Fields, and Vector Spaces: An Approach to Geometric Constructability.
Shores: Applied Linear Algebra and Matrix Analysis.
Sigler: Algebra.
Silverman/Tate: Rational Points on Elliptic Curves.
Simmonds: A Brief on Tensor Analysis. Second edition.
Singer: Geometry: Plane and Fancy.
Singer: Linearity, Symmetry, and Prediction in the Hydrogen Atom.
Singer/Thorpe: Lecture Notes on Elementary Topology and Geometry.
Smith: Linear Algebra. Third edition.
Smith: Primer of Modern Analysis. Second edition.
Stanton/White: Constructive Combinatorics.
Stillwell: Elements of Algebra: Geometry, Numbers, Equations.
Stillwell: Elements of Number Theory.
Stillwell: The Four Pillars of Geometry.
Stillwell: Mathematics and Its History. Second edition.
Stillwell: Naive Lie Theory.
Stillwell: Numbers and Geometry. *Readings in Mathematics.*
Strayer: Linear Programming and Its Applications.
Toth: Glimpses of Algebra and Geometry. Second Edition. *Readings in Mathematics.*
Troutman: Variational Calculus and Optimal Control. Second edition.
Valenza: Linear Algebra: An Introduction to Abstract Mathematics.
Whyburn/Duda: Dynamic Topology.
Wilson: Much Ado About Calculus.