Additional Problems for *An Invitation to Modern Number Theory*

Steven J. Miller* and Ramin Takloo-Bighash†

June 16, 2007

Abstract

Below are some addition problems for *An Invitation to Modern Number Theory*. For more information, see the book's homepage at

`http://www.math.princeton.edu/mathlab/book/index.html`.

This list will be updated as new problems are added.

1 Chapter 1: Mod p Arithmetic, Group Theory and Cryptography

From §1.2: Let $f(x) = x^2 - a$. Show that we may write x_{n+1} as

$$x_{n+1} \ = \ \frac{1}{2}\left(x_n + \frac{a}{x_n}\right). \tag{1.1}$$

Find a similar formula for $g(x) = x^p - a$.

From §1.3: Let $x = 2^n + 1$ be a prime. Prove $n = 2^m$ for some m. Primes of the form $2^{2^n} + 1$ are called Fermat primes.

From §1.4.2: Let $p < q$ be two distinct odd primes. Prove $p + p^2 + \cdots + p^{q-1} \equiv 0 \bmod pq$. For what p and q is $q + q^2 + \cdots + q^{p-1} \equiv 0 \bmod pq$?

From §1.5: If N is the product of two distinct odd primes, show that at least one out of every three consecutive integers is relative prime to N. Thus if the last digit of a message is kept free, it is always possible to choose a final digit so that the message is relatively prime to N.

*E-mail: `sjmiller@math.brown.edu`
†E-mail: `rtakloo@math.princeton.edu`

From §1.5: It is essential that e is relatively prime to $\phi(pq) = (p-1)(q-1)$. Unlike the above exercise, show it is possible for three consecutive numbers not to be relatively prime to $\phi(pq)$; how many consecutive numbers can share a factor with $\phi(pq)$? The answer will depend on the prime factorizations of $p-1$ and $q-1$. In the remarks to this exercise we discuss how if p and q are Germain primes then one out of every six consecutive integers are relative prime to $\phi(pq)$.

2 Chapter 2: Arithmetic Functions

§2.3.1: The following observation (see F. Saidak, *A new proof of Euclid's theorem*, Amer. Math. Monthly **113** (2006), no. 10, 937–938) leads to another proof of the infinitude of primes: if $n > 1$ then n and $n+1$ are relatively prime (i.e., the only integer dividing both is 1). Prove this assertion, and then deduce there must be infinitely many primes by showing a_n is divisible by at least 2 distinct primes, where $a_2 = 2 \cdot 3$ and $a_{n+1} = a_n \cdot (a_n + 1)$. Similar to the previous exercise, what kind of bounds can you find for the size of $\pi(x)$ using these arguments?

3 Chapter 3: Zeta and L-Functions

4 Chapter 4: Solutions to Diophantine Equations

5 Chapter 5: Algebraic and Transcendental Numbers

From §5.3: Consider N points in the plane. For each point, color every point an irrational distance from that point blue. What is the smallest N needed such that, if the points are properly chosen, every point in the plane is colored blue? If possible, give a constructive solution (i.e., give the coordinates of the points).

From §5.4: Split 100 into smaller integers such that each integer is two or more and the product of all these integers is as large as possible. Suppose now N is a large number and we wish to split N into smaller pieces, but all we require is that each piece be positive. How should we break up a large N?

From §5.4: Without using a calculator or computer, determine which is larger: e^π or π^e.

6 Chapter 6: The Proof of Roth's Theorem

7 Chapter 7: Introduction to Continued Fractions

From §5.2.2: Let $p/q \in (0, 2]$ be a rational number. Prove it may be written as a sum of distinct rationals of the form $1/n$ (for example, $31/30 = 1/2 + 1/3 + 1/5$). (*Hard:* is the claim still true if $p/q > 2$?).

From §7.3.1: Zeckendorf's Theorem: Consider the set of distinct Fibonacci numbers: $\{1, 2, 3, 5, 8, 13, \dots\}$. Show every positive integer can be written uniquely as a sum of distinct Fibonacci numbers where we do not allow two consecutive Fibonacci numbers to occur in the decomposition. Equivalently, for any n there are choices of $\epsilon_i(n) \in \{0, 1\}$ such that

$$n \;=\; \sum_{i=2}^{\ell(n)} \epsilon_i(n) F_i, \quad \epsilon_i(n)\epsilon_{i+1}(n) = 0 \text{ for } i \in \{2, \dots, \ell(n) - 1\}. \tag{7.1}$$

Does a similar result hold for all recurrence relations? If not, can you find another recurrence relation where such a result holds?

8 Chapter 8: Introduction to Probability

From §8.1.2: Alan and Barbara take turns shooting a basketball; first one to make a basket wins. Assume every time Alan shoots he has a probability $p \in [0, 1]$ of making a basket, and each time Barbara shoots she has a probability $q \in [0, 1]$ of making a basket. For notational convenience let $r = (1-p)(1-q)$. We assume that at least one of p and q is positive (as otherwise the game never ends); thus $r \in [0, 1)$. The probability that Alan wins on his first shot is p, that he wins on his second shot is rp (he must miss his first shot, Barbara must miss her first shot, and then he must make his second shot), and in general that he wins on his n^{th} shot is $r^{n-1}p$. Letting x equal the probability that Alan wins, we find

$$x \;=\; p + rp + r^2p + \cdots \;=\; p\sum_{n=0}^{\infty} r^n. \tag{8.1}$$

However, we also know that

$$x \;=\; p + (1-p)(1-q)x \;=\; p + rx. \tag{8.2}$$

This follows from observing that, once Alan and Barbara miss their first shots, it is as if we started the game all over; thus the probability that Alan wins after they each miss their first shot is the same as the probability that Alan wins (we must remember to add on the probability that Alan wins on his first shot, which is p). Since $x = p + rx$ we find $x = p/(1-r)$, so (8.1) becomes

$$\sum_{n=0}^{\infty} r^n \;=\; \frac{1}{1-r}, \tag{8.3}$$

the geometric series formula!

From §8.1.6: Consider a group of m people. We choose a person at random (thus each person is equally likely to be chosen); we do this n times (at each step, each person is equally likely to be chosen). If $n < m$ then clearly there is at least one person whom we haven't chosen. How large must n be so that we have a 50% chance of having chosen everyone at least once? What is the average value of n such that everyone is chosen at

least once? See the remarks for applications.

From §8.1.6: Does there exist a probability distribution such that Chebyshev's Inequality is an equality for all positive integral k?

From §8.2.1: The above example provides a proof for the geometric series formula, but only if $r \in [0,1)$. If $r < 0$ show how we may deduce the geometric series formula from the $r \geq 0$ case.

From §8.2.1: Alan and Barbara now play the following game. Alan starts with n dollars and Barbara with m dollars (n and m are positive integers). They flip a fair coin and every time they get heads Barbara pays Alan a dollar, while every time they get a tail Alan pays Barbara a dollar. They continue playing this game until one of them has all the money. Prove the following:

1. If $n = m$ then the probability that Alan wins is $n/(n+m) = 1/2$.
2. If $n+m = 2^k$ for some positive k then the probability that Alan wins is $n/(n+m)$.
3. If $m = 2$ then the probability that Alan wins is $n/(n+m)$, and if $m = 1$ then the probability that Alan wins is $n/(n+m)$.
4. For $1 \leq m, n$ the probability that Alan wins is $n/(n+m)$.

Investigate what happens for small m and n if the coin is *not* fair.

From §8.2.1: Consider a circle of unit radius and a square of diameter 2. Assume we paint p percent of the perimeter blue and $1-p$ of the perimeter red. Prove that if $p < 1/4$ then there *must* be a way to position the square inside the circle so that the four vertices are on the perimeter and all four vertices are on the red parts of the circle. Generalize the problem to an n dimensions.

From §8.2.1: Consider the normal distribution with mean 0 and variance σ^2; its density is $f(x;\sigma) = (2\pi\sigma^2)^{-\frac{1}{2}} e^{-x^2/2\sigma^2}$. As $f(x;\sigma)$ integrates to 1, we have

$$\sigma \;=\; \int_{-\infty}^{\infty} \frac{e^{-x^2/2\sigma^2}}{\sqrt{2\pi}}\, dx. \tag{8.4}$$

By differentiating with respect to σ, show the second moment (and hence the variance since the mean is zero) is σ^2. This argument may be generalized (it may be easier to consider the operator $\sigma^3 d/d\sigma$) and yields all even moments of the Gaussian; the $2m^{\text{th}}$ moment is $(2m-1)(2m-3)\cdots 3\cdot 1\cdot \sigma^{2m}$ and is often denoted $(2m-1)!!$ (here the double factorial means every other term; thus $7!! = 7\cdot 5\cdot 3\cdot 1$ and $6!! = 6\cdot 4\cdot 2$).

From §8.2.1: The even moments of the Gaussian (see the above exercise) have an interesting combinatorial meaning. Show that the number of ways of pairing $2m$ objects into m pairs of two elements is $(2m-1)!!$. We shall see these moments again when we study the eigenvalues of real symmetric Toeplitz matrices.

9 Chapter 9: Applications of Probability: Benford's Law and Hypothesis Testing

From §9.1: Below we use the following definition of the $3x+1$ map:

$$a_{n+1} = \frac{3a_n+1}{2^k}, \tag{9.1}$$

Show there are arbitrarily large integers N such that if $a_0 = N$ then $a_1 = 1$. Thus, infinitely often, one iteration is enough to enter the repeating cycle. More generally, for each positive integer k does there exist arbitrarily large integers N such that if $a_0 = N$ then $a_j > 1$ for $j < k$ and $a_k = 1$?

10 Chapter 10: Distribution of Digits of Continued Fractions

From §10.3: Show that the number $\log_2\left(1+\frac{1}{k(k+2)}\right)$ are non-negative and sum to 1. Thus it is reasonable to call these numbers probabilities.

11 Chapter 11: Introduction to Fourier Analysis

12 Chapter 12: $\{n^k\alpha\}$ and Poissonian Behavior

From §12.2: Let α be an irrational number, and let $x_n = 2^n\alpha \bmod 1$. Must $\{x_n\}_{n\in\mathbb{N}}$ be dense?

13 Chapter 13: Introduction to the Circle Method

14 Chapter 14: Circle Method: Heuristics for Germain Primes

15 Chapter 15: From Nuclear Physics to L-Functions

From §15.2.1: Find formulas for $\lambda_1(A)$ and $\lambda_2(A)$ for 2×2 matrices in terms of Trace(A) and Trace(A^2).

16 Chapter 16: Random Matrix Theory: Eigenvalue Densities

17 Chapter 17: Random Matrix Theory: Spacings between Adjacent Eigenvalues

From §17.2.3: Consider 3×3 real symmetric matrices with each entry chosen independently from a fixed probability distribution. There are thus 6 independent variables: a_{11}, a_{12}, a_{13}, a_{22}, a_{23}, and a_{33}. The three eigenvalues $\lambda_1(A), \lambda_2(A)$ and $\lambda_3(A)$ are thus functions of these six parameters. Calculate how many degrees of freedom there are if two of the eigenvalues are equal. *Hint: if α is a repeated root of $f(x)$, then $f(\alpha) = 0$ and $f'(\alpha) = 0$. Let $f(\lambda) = \det(\lambda I - A)$. As the characteristic polynomial is a cubic, to have a repeated root α we must have $f(\alpha) = f'(\alpha) = 0$. As f' is a quadratic, we can find its roots by using the quadratic formula.*

From §17.2.3: In the spirit of the above remark, consider the quadratic equations $f_{a,b,c}(x) = ax^2 + bx + c = 0$, $a, b, c \in \{0, \dots, N-1\}$. There are N^3 such quadratics. As $N \to \infty$, as a function of N approximately how many of these polynomials have repeated roots?

18 Chapter 18: The Explicit Formula and Density Conjectures