4400/6400 EXERCISES

PETE L. CLARK

1. Homework 1

1.1. 4400 Problems.

Exercise 1.1.1. (O)[1] How do you know there is no largest integer?

Exercise 1.1.2. We recall the definition of divisibility in $\mathbb{Z}$: if $a, b \in \mathbb{Z}$ we say that **a divides b** and write $a \mid b$ if there is $c \in \mathbb{Z}$ such that $ac = b$.
a) Show: if $a \in \mathbb{Z}$, then $a \mid 0$.
b) Show: if $a \in \mathbb{Z}$ and $0 \mid a$, then $a = 0$.
c) Suppose $a, b, c \in \mathbb{Z}$ and that we have $a \mid b$ and $a \mid c$. Show: $a \mid b + c$. In fact, show that for all $x, y \in \mathbb{Z}$, we have $a \mid bx + cy$.
d) Suppose that $a, b, c \in \mathbb{Z}$, that $a \mid b$ and $a \nmid c$ (i.e., a does not divide c.) Show: $a \nmid b + c$.
e) Suppose $a, b, c \in \mathbb{Z}$ and that $a \nmid b$ and $a \nmid c$. What can we conclude about whether $a \mid b + c$? (If anything, prove it. If not, give examples to show that.)

Exercise 1.1.3. We can extend the definition of divisibility from $\mathbb{Z}$ to any commutative ring R: if $a, b \in R$ we say that **a divides b** and write $a \mid b$ if there is $c \in \mathbb{R}$ such that $ac = b$.
a) Which of the parts of the previous problem continue to hold in any commutative ring? In any integral domain?
b) For $a \in R$, we define the **principal ideal**

$$(a) = \{xa \mid x \in R\}.$$

Show: for $a, b \in R$, we have $a \mid b \iff (a) \supset (b)$. ("To contain is to divide.")

Exercise 1.1.4. Recall that a relation $\leq$ on a set X is a **partial ordering** if it satisfies all of the following properties:
(PO1) (Reflexivity) For all $x \in X$, we have $x \leq x$.
(PO2) (Anti-symmetry) For all $x, y \in X$, if $x \leq y$ and $y \leq x$, then $x = y$.
(PO3) (Transitivity) For all $x, y, z \in X$, if $x \leq y$ and $y \leq z$ then $x \leq z$.
A partial ordering is **total** if it moreover satisfies
(PO4) (Totality) For all $x, y \in X$, either $x \leq y$.
The usual $\leq$ is a total ordering on $\mathbb{Z}$. (Not asking you to show this!)
Check which of the four axioms above are satisfied for the divisibility relation $\mid$ on $\mathbb{Z}$, on $\mathbb{N}$ and on $\mathbb{Z}^+$.

Exercise 1.1.5. Recall Euclid's Lemma: if p is a prime number and $a, b \in \mathbb{Z}$, then $p \mid ab \implies p \mid a$ or $p \mid b$.
a) Show: if $a_1, \ldots, a_n \in \mathbb{Z}$ and $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for at least one i.

[1] A problem marked (O) is "open-ended." Think of it as a discussion rather than a right or wrong answer.

b) Show the **Generalized Euclid's Lemma**: suppose $a, b, c \in \mathbb{Z}$, that $a \mid bc$ and $\gcd(a, b) = 1$. Show: $a \mid c$.
(Suggestion: use the Fundamental Theorem!)

Exercise 1.1.6. An **arithmetic progression** (in $\mathbb{Z}$) is a finite or infinite sequence of integers such that the difference of any two consecutive terms is constant. Thus an arithmetic progression is determined by the initial value $a_0 \in \mathbb{Z}$, the **common difference** $d \in \mathbb{Z}^+$ and the **length** $k \leq \infty$, so if $k < \infty$, the progression looks like

$$a_0,\ a_1 = a_0 + d,\ a_3 = a_0 + 2d, \ldots, a_{k-1} = a_1 + (k-1)d$$

and if $k = \infty$ it looks similarly but goes on forever.

In this exercise we are interested in arithmetic progressions in which each term is a prime number; we call these **PAP**'s. If the length is k, we speak of a k-PAP.
a) Check that $5, 11, 17, 23, 29$ is a 5-PAP.
b) Find a 6-PAP. (Suggestion: start with a prime a_0 and a common difference d such that $a_0 + d$ is prime, and then see how many prime value you get. I.e., just experiment. You will soon see that the choice of d is much more important than the choice of a_0.)
c) Show: $3, 13, 23$ is the only 3-PAP with $d = 10$.
d) Show in any 6-PAP the common difference d must be divisible by 30.
e) Let $a, a + d, \ldots, a + (k-1)d$ be a k-PAP. Show: $p \mid d$ for all primes $p \leq \frac{k}{2}$.
f) Deduce from part e) that there is no *infinite* PAP.
g)$*$ Show: if $a, a + d, \ldots, a + (k-1)d$ is a k-PAP, then every prime $p < k$ divides d. Show by example that this cannot be improved to: every prime $p \leq k$ divides d.
h) When I first taught this course, the largest k for which there was an *explicitly known* k-PAP was $k = 23$. Is this still the case?

Exercise 1.1.7. a) Let $N \in \mathbb{Z}^+$ and write it as $10a + b$ (i.e., b is the final decimal digit of N). Show that $7 \mid N \iff 7 \mid a - 2b$. Explain why this gives an test for divisibility by 7.
b) Can you find a similar test for divisibility by 13?
c) (O): Prove: For every positive integer d, there is a test for divisibility by d.

Commentary on part c): Exactly what a "divisibility by d" test means is part of what you have to figure out. Of course we could always use the division algorithm we learned in elementary school, so presumably a divisibility test is something that is faster and/or easier than this. That some divisibility tests are faster and easier than actual division is pretty obvious: for instance, to test divisibility by 125 we only need to see if the last three digits are any of 125, 250, 375, 500, 625, 750, 875 or 000. The test for divisibility by 7 that comes from part a) is not as fast as that. Also, this is the rare problem where it is important that N is given to us as its decimal expansion. If we were allowed to rewrite N in base d notation, the teset would be trivial.

Exercise 1.1.8. Try to formulate a conjecture on when a polynomial with integer coefficients represents infinitely many primes. If you want to look this one up, the keyword is **Schinzel's Hypothesis**.

Exercise 1.1.9. $*$ Let $p(x)$ be a nonconstant polynomial with integer coefficients. Show that there are infinitely many positive integers n such that $p(n)$ is *not* prime.

Exercise 1.1.10. The term "polynomial function on the integers" is ambiguous. On the one hand we could mean a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

with all $a_i \in \mathbb{Z}$. On the other hand, we could mean that the coefficients a_i are real numbers, but nevertheless for all $n \in \mathbb{Z}$, $P(n) \in \mathbb{Z}$: i.e., as a function we have $P(\mathbb{Z}) \subset \mathbb{Z}$. Let us call this latter condition **integer-vlaued**. a) Show that $P_2(x) = \frac{1}{2}x^2 + \frac{1}{2}x$ is integer-valued but does not have integer coefficients.
b) Show that an integer-valued function has *rational coefficients*. (Suggestion: Lagrange Interpolation Formula.)
c)$*$ Find an explicit description of all integer-valued polynomials of degree d. For instance, any quadratic integer-valued polynomial is of the form $ap_2(x) + bx + c$ for $a, b, c \in c$. (Hint: think about binomial coefficients.)

Exercise 1.1.11. **Schuh's divisor game** is played as follows: we begin with a positive integer N and all of its positive divisors. Two players play, alternating turns. On a given turn, a player chooses a positive divisor d of N and *takes* that divisor and also all of *its* positive divisors $e \mid d$. The game ends when all the divisors of N should be taken.
a) I haven't told you who wins the game! Should the player who makes the last move win or lose? (One way makes a really boring game.)
b) For a given value of N, there must be a winning strategy for either the first player or the second player: why?
c) Analyze the game for small values of N. You will find that the game does not depend on the numerical values but rather on the shape of the prime factorization of N. Find explicit winning strategies when N is
(i) p^a (a power of a prime)
(ii) pq (a product of two distinct primes)
(iii) pqr (a product of three distinct primes)
d)$*$ Show: for any $N > 1$, the first player has a winning strategy. Note here that you are not being asked for a *specific* winning strategy for all N: in fact that is not known. (Hint: suppose for the sake of argument that the second player has a winning strategy. Figure out how the first player can "steal" it.)
e)$*$ Write a computer program that will play Schuh's divisor game.

1.2. **6400 Problems.**

Exercise 1.2.1. A **monoid** is a set M equipped with a binary operation $\star : M \times M \to M$ that is associative and has a two-sided identity:

$$\exists e \in M \mid \forall m \in M \ e \star m = m \star e = m.$$

(Thus a monoid in which each element has an inverse is precisely a group.) Monoids need not be commutative, but they will be in this problem.
a) Observe: $(\mathbb{N}, +)$ the natural numbers under addition, form a commutative monoid, as does $(\mathbb{Z}^+, \cdot)$, the positive integers under multiplication.
b) Generalizing what we did with these two monoids, in our commutative monoid M we introduce a relation $\mathcal{R}$: namely $a\mathcal{R}b$ iff there is $c \in M$ such that $a \star c = b$. So that this relation is reflexive and transitive, but in general it need not be antisymmetric. (Hint: try a nontrivial group.) Such a relation is called a **quasi-order**.
c) The two monoids $(\mathbb{N}, +)$ and $(\mathbb{Z}^+, \cdot)$ have further nice properties:
(P1) Cancellation: if $a \star b = a \star c$, then $b = c$.

(P2) Reducedness: if $a \star b = e$, then $a = b = e$.
Show: that in any commutative monoid satisfying (P1) and (P2), the relation $\mathcal{R}$ above is a partial ordering.
d) Given commutative monoids $(M, +)$ and $(N, +)$, we introduce the **direct sum** $M \oplus N$: as a set it is just the Cartesian product, i.e., its elements are ordered pairs (m, n) with $m \in M$ and $n \in N$. The operation is "componentwise":

$$(m_1, n_1) + (m_2, n_2) \coloneqq (m_1 + m_2, n_1 + n_2).$$

Show: If M and N each satisfy (P1) and (P2), so does $M \oplus N$. If so, show that the resulting partial order is also componentwise: $(m_1, n_1)\mathcal{R}(m_2, n_2)$ iff $m_1 \mathcal{R} m_2$ and $n_1 \mathcal{R} n_2$. Deduce: if M and N each have more than one element, this partial order is not a total order.
e) Show that $(\mathbb{N}, +) \oplus (\mathbb{N}, +)$ is isomorphic to the submonoid of $(\mathbb{Z}^+, \cdot)$ of the form $p^a q^b$ for (any) two distinct primes p and q.
f) Given an infinite indexed family $\{M_i\}_{i \in I}$ of comutative monoids, we define the direct sum $\bigoplus_{i \in I} M_i$ to the subset of the Cartesian product $\prod_{i \in I} M_i$ consisting of tuples $\{e_i\}$ such that $e_i = 0$ (the identity in M_i) for all but finitely many i. Show: that the direct sum of a countably infinite number of copies of $(\mathbb{N}, +)$ with itself is isomorphic to the multiplicative monoid $(\mathbb{Z}^+, \cdot)$.
(This formalizes the statement that the primes are the building blocks of $\mathbb{Z}^+$ under multiplication, just as 1 is the single building block of $\mathbb{N}$ under addition.)
g)$*$ The process of forming the integers from the natural numbers and the rational numbers from the integers can be generalized to get a group out of commutative monoid. Namely, for a commutative monoid $(M, +)$, let $G'(M)$ be the set of all ordered pairs $(p, m) \in M \oplus M$, and consider the following equivalence relation on $G'(M)$: $(p_1, m_1) \sim (p_2, m_2)$ iff there is $s \in M$ such that $s + p_1 + m_2 = s + p_2 + m_1$. Show that the operation on $M \oplus M$ is well-defined on $\sim$ equivalence classes and endows it with the structure of a commutative group, in which the inverse of the class $[(p, m)]$ is the class $[(m, p)]$.
(This group is denoted $G(M)$ and called the **group completion** or **Grothendieck group** associated to M.)

Exercise 1.2.2. Let $(S, \leq)$ be a finite partially ordered set with a bottom element e – i.e., $e \leq s$ for all $s \in S$. We can play the **poset game** on S: players alternate turns. On each turn, a player chooses an element $s \in S$; they then remove that element and also all elements $t \leq s$. The player who moves last loses.
a) Explain how the poset game generalizes Schuh's divisor game.
b) Either prove that the first player alwys has a win, or give a counterexample. (The trivial case in which $S = \{e\}$ does not count as a counterxample!)
c) The poset game is the subject of an award-winning high school science project of Steven Byrnes. What is Byrnes' Poset Game Periodicity Theorem?

2. Homework 2

2.1. 4400 Problems.

Exercise 2.1.1. Prove the **Division Theorem**: for any $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, there are unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.

Exercise 2.1.2. For integers x, y, a **greatest common divisor** is an integer d such that $d \mid x$, $d \mid y$, and for any integer e such that $e \mid x$ and $e \mid y$, then $e \mid d$.

(Here it is important to understand that "greatest" is with respect to the relation of divisibility, *not* necessarily the usual $\leq$ coming from the additive structure.)
a) Show that if d is a greatest common divisor of x and y, so is $-d$.
b) Show that 0 is a greatest common divisor of 0 and 0 and moreover that it is the only greatest common divisor.
c) Show: if $x, y \in \mathbb{Z}$ are not both zero, then there are exactly two greatest common divisors of x and y: a positive integer d and its negative $-d$. By convention, when we write $\gcd(x, y)$, we usually mean the unique positive one.

Exercise 2.1.3. Let R be a commutative ring. Recall that an **ideal** I is a subset of R such that
(I1) For all $x, y \in I$ we have $-x \in I$ and $x + y \in I$.
(That is, I is a subgroup of the additive group $(R, +)$).
(I2) for all $x \in I$ and all $r \in R$, we have $rx \in I$.
a) Let $x_1, \ldots, x_n$ be any elements of R. We define

$$(x_1, \ldots, x_n) \coloneqq \{r_1 x_1 + \ldots + r_n x_n \mid r_1, \ldots, r_n \in R\}.$$

Show that this is an ideal of R. It is called "the ideal generated by $x_1, \ldots, x_n$."
b) When $n = 1$ we simply get the ideal (x_1) of all multiples of x_1. Such ideals are called principal. A **principal ideal domain (or PID)** is an integral domain in which every ideal is principal. In class we showed that $\mathbb{Z}$ is a PID. Let R be any PID, let $x_1, \ldots, x_n \in R$. Then by definition there is $d \in R$ such that

$$(x_1, \ldots, x_n) = (r).$$

Show that r is a **greatest common divisor** of $x_1, \ldots, x_n$: that is, $r \mid x_i$ for all i and if $s \mid x_i$ for all i then $s \mid r$.
c) In number theory it is common to denote the greatest common divisor of integers $x_1, \ldots, x_n$ by $(x_1, \ldots, x_n)$. In our notation, this is the ideal generated by $x_1, \ldots, x_n$. Explain why these two notational choices are almost compatible.

Exercise 2.1.4. Let $a, b \in \mathbb{Z}$.
a) Show that for all $x \in \mathbb{Z}$, we have $(a, b) = (a + xb, b)$.
b)$*$ Show that part a) holds verbatim with $\mathbb{Z}$ replaced by any commutative ring R.
c) Suppose $b \in \mathbb{Z}^+$, and write $a = qb + r$ as in the Division Theorem. Deduce from part a) that

$$(a, b) = (b, r).$$

d) Explain the **Euclidean Algorithm** for computing the gcd of two positive integers in terms of part c).

Exercise 2.1.5. Let $\mathbf{E}$ be the *rng* of all even integers. Give a necessary and sufficient condition on a positive element $x \in \mathbf{E}$ to have two different factorizations into positive $\mathbf{E}$-primes.
(Hint: pay attention to $\mathrm{ord}_2(x)$ and to the number of odd primes dividing x.)

Exercise 2.1.6. Complete the proof of the fact that for all $n \geq 2$, the harmonic sum

$$H_n = \sum_{i=1}^{n} \frac{1}{i}$$

is not an integer by showing that for all $n \in \mathbb{Z}^+$ we have $\mathrm{ord}_2 H_n \neq \mathrm{ord}_2 \frac{1}{n+1}$.

Exercise 2.1.7. $**$ Show that except for $n = 1, 2, 6$, we have $\mathrm{ord}_p(H_n) < 0$ for some prime $p \neq 2, 5$.

Exercise 2.1.8. a) Show that if I and J are ideals in a commutative ring, then $I \cap J$ is also an ideal.
b) Let $a, b \in \mathbb{Z}^+$. By part a), $(a) \cap (b)$ is an ideal in $\mathbb{Z}$. But because $\mathbb{Z}$ is a PID, we must have $(a) \cap (b) = (c)$ for some $c \in \mathbb{Z}^+$. What is c in terms of a and b?

Exercise 2.1.9. a) Show: for $a, b \in \mathbb{Z}^+$ we have $\gcd(a, b) \operatorname{lcm}(a, b) = ab$.
b) $*$ Let $a, b, c \in \mathbb{Z}^+$. Find an identity relating $\gcd(a, b, c)$, $\operatorname{lcm}(a, b, c)$ and abc. What if there are more than three numbers? (Suggestion: use inclusion/exclusion.)

Exercise 2.1.10. One says that integers $a_1, \ldots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ for all $i \neq j$.
a) Show: if $a_1, \ldots, a_n$ are pairwise relatively prime then $\gcd(a_1, \ldots, a_n) = 1$.
b) Show that the converse does not hold when $n \geq 3$. Indeed, find the smallest example of three positive integers not simultaneously divisible by any $d > 1$ but for which any 2 have a nontrivial common divisor.

Remark: The phrase "Let $a_1, \ldots, a_n$ be relatively prime integers" is therefore ambiguous when $n \geq 3$. If you are not sure which meaning is intended, stop and ask!

Exercise 2.1.11. a) Prove the **Rational Roots Theorem**: if

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

is a polynomial with integer coefficients and $a_n \neq 0$, then the only possible rational roots are of the form $\pm \frac{c}{d}$ where $c \mid a_0$ and $d \mid a_n$.
b) In particular, if $a_n = 1$ – one says that P is **monic** – then every rational root of P is an integer.
c) Use either part a) or part b) to give a very quick proof of the irrationality of $\sqrt{2}$.

Exercise 2.1.12. a) Show that $\log_2 10$ is irrational.
b)$*$ Let $a, b \in \mathbb{Z}^+$. Give a criterion for the irrationality of $\log_a b$.

2.2. **6400 Problems.**

3. Homework 3

3.1. **4400 Problems.**

Exercise 3.1.1. Let $N \in \mathbb{Z}^+$. A **primitive root modulo N** is an integer g such that for every $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, there is $n \in \mathbb{Z}$ such that $g^n = x$. In more algebraic terms, it is a generator of the group $(\mathbb{Z}/N\mathbb{Z})^\times$, and it exists whenever the group is cyclic.
a) Show that g is a primitive root modulo N iff for $n \in \mathbb{Z}^+$, if $g^n \equiv 1 \pmod{N}$ then $n \geq \varphi(N)$.
b) Using your criterion of part a), for each $2 \leq N \leq 32$ either find a primitive root modulo N or show that no primitive roots exist.

Exercise 3.1.2. * Find all integers x, y, z such that $3x + 4y + 5z = 1$.
(Suggestion: the matter of it is to find all solutions to the associated homogeneous equation $3x + 4y + 5z = 0$. To do this: for any $x \in \mathbb{Z}$, we are trying to find all $y, z \in \mathbb{Z}$ such that $4y + 5z = -3x$. It is no problem to find a $\mathbb{Q}$-basis for all $\mathbb{Q}$-solutions to this equation: e.g. take $(-4/3, 1, 0)$ and $(-5/3, 0, 1)$, so the general $\mathbb{Q}$-solution is $\{(-4/3b + 5/3c, b, c) \mid b, c \in \mathbb{Q}\}$. The tricky part is finding a $\mathbb{Z}$-basis for all $\mathbb{Z}$-solutions: for instance, clearly $(-4, 3, 0)$ and $(-5, 0, 3)$ are $\mathbb{Z}$-solutions, but not every $\mathbb{Z}$-solution is of the form $(-4B - 5C, 3B, 3C)$ for $B, C \in \mathbb{Z}$.)

Exercise 3.1.3. Let $m, b \in \mathbb{R}$, and consider the line

$$\ell : y = mx + b.$$

Let $\mathcal{S} = \{(x, y) \in \mathbb{Q}^2 \mid y = mx + b\}$ be the set of $\mathbb{Q}$-rational points on ℓ.
a) Show: either $\mathcal{S}$ is empty or $\mathcal{S}$ consists of exactly one point or $\mathcal{S}$ is infinite.
b) Show: if $m, b \in \mathbb{Q}$, then $\mathcal{S}$ is infinite.
c) Show: if $m \in \mathbb{Q}$ and $b \notin \mathbb{Q}$, then $\mathcal{S} = \varnothing$.
d) Show: if $m \notin \mathbb{Q}$ and $b \in \mathbb{Q}$, then $\#\mathcal{S} = 1$.
e) What can be said if $m, b \notin \mathbb{Q}$?

Exercise 3.1.4. Let a and b be relatively prime positive integers.
a) Show: there *do not* exist $x, y \in \mathbb{N}$ such that $xa + yb = ab - a - b$.
b) Show: for all $N > ab - a - b$, there are $x, y \in N$ such that $xa + yb = N$.

Exercise 3.1.5. It used to be the case that Chicken McNuggets were sold in packs of 6, 9 and 20. Assuming this: what is the largest number of Chicken McNuggets you *cannot* buy?
(It is not obvious that such a largest number exists...but it does.)

Exercise 3.1.6. Let $c, N \in \mathbb{Z}$ with $N > 1$. Let $\overline{c}$ be the class of c modulo N.
a) Show: $\overline{c} \in (\mathbb{Z}/N\mathbb{Z})^\times$ iff $\gcd(c, N) = 1$.
b) Recall that $\varphi(N) \coloneqq \#(\mathbb{Z}/N\mathbb{Z})^\times$. Show: $\varphi(N) \leq N - 1$ and that equality holds iff N is prime.

Exercise 3.1.7. Lagrange's Theorem in group theory says that if G is a finite group and H is a subgroup then $\#H \mid \#G$. (Appendix A of the course text contains a proof.) For number-theoretic purposes one can usually get away with the following easier result:

Lagrange's Little Theorem: Let $(G, \cdot)$ be a finite commutative group, and let $g \in G$. Then the order of g – the least $n \in \mathbb{Z}^+$ such that $g^n = 1$ – divides $\#G$.
a) Fill in the following sketch proof of **Lagrange's Little Theorem**: say $N = \#G$, and write out the elements of G in some order as $x_1, \ldots, x_N$. Let

$$P \coloneqq \prod_{i=1}^{N} x_i.$$

Show that also

$$P = \prod_{i=1}^{N} g x_i,$$

and deduce that $g^N = e$ (the identity element of G).
b) Deduce **Fermat's Little Theorem**: for $x \in \mathbb{Z}$ and p a prime number, we have $x^p \equiv x \pmod{p}$.

Exercise 3.1.8. Fill in the details of the following sketch proof of **Wilson's Theorem**: for any prime number p, we have $(p-1)! \equiv -1 \pmod{p}$. First we observe that we are trying to evaluate the product $P \coloneqq \prod_{i=1}^{p-1} x_i$ of the previous exercise when G is the group $(\mathbb{Z}/p\mathbb{Z})^\times$. Now let $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. If $x \neq x^{-1}$, then x and x^{-1} both appear in the product in question, and they cancel each other out. Therefore P is actually equal to the product of all $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ that are self-inverse. But the only such elements are 1 and -1 (be sure to explain why!), and thus $P = 1 \cdot -1 = -1$.

Exercise 3.1.9. Let p be a prime number.
a) Show the following polynomial identity in $\mathbb{Z}/p\mathbb{Z}[X]$:

$$X^{p-1} - 1 = (X-1)(X-2)\cdots(X-(p-1)).$$

(Suggestion: use Fermat's Little Theorem and the Root-Factor Theorem.)
b) Evaluate the above identity at $X = 0$ and get another proof of Wilson's Theorem.

Exercise 3.1.10. * The above exercises raise the question of the value of the product $P = \prod_{x \in G} x$ for an arbitrary finite commutative group G. Prove: if G has exactly one element, say t, of order 2, then $P = t$; otherwise $P = 1$.

3.2. **6400 Problems.**

Exercise 3.2.1. Let R be a ring, let I be an ideal of R. Let $c \in R$, and write $\overline{c}$ for the class of c in R/I. Show that $c \in (R/I)^\times$ iff the ideal

$$(c, I) := \{rc + i \mid r \in R,\ i \in I\}$$

is all of R. Explain why this generalizes Exercise 3.1.6a).

Exercise 3.2.2. Fill in the details of the following sketch proof of Wilson's Theorem (due to Gerrish): let p be a prime number.
a) Show that the Sylow subgroups of the symmetric group S_p are cyclic of order p.
b) Show that the number of Sylow p-subgroups of S_p is $n_p = (p-2)!$.
(Hint: count the number of p-cycles in S_n and divide by the number of generators of a cyclic group of order p.)
c) By the Sylow Theorems we have $n_p \equiv 1 \pmod{p}$, so $(p-1)n_p = (p-1)! \equiv (p-1) \equiv -1 \pmod{p}$.

4. Homework 4

4.1. **4400 Problems.**

Exercise 4.1.1. Please read up on the following aspects of factorization in integral domains, either from the course text or from the beginning of `http://alpha.math.uga.edu/~pete/factorization2010.pdf`. Check your reading by answering the following as true or false (you don't need to give proofs):
a) Every prime element in a domain is irreducible.
b) Every irreducible element in a domain is prime.
c) Every principal ideal domain is a unique factorization domain.

Exercise 4.1.2. Let $D \in \mathbb{Z}$, and let p be a prime number. Show that if there are integers $x, y \in \mathbb{Z}$ such that $x^2 - Dy^2 = p$, then D is a square modulo p.

Exercise 4.1.3. Let $D \notin \{0, 1\}$ be a squarefree integer, and let $\mathbb{Q}(\sqrt{D})$ be the corresponding quadratic field. Define the conjugation map

$$\alpha = a + b\sqrt{D} \mapsto \overline{\alpha} = a - b\sqrt{D}$$

and the **norm map**

$$N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q},\ \alpha \mapsto N(\alpha) = \alpha\overline{\alpha}.$$

a) Show that conjugation is a field isomorphism: i.e., a bijection that preserves addition and multiplication.
b) Show that $N(a + b\sqrt{D}) = a^2 - Db^2$.

c) Show that $N : \mathbb{Q}(\sqrt{D})^\times \to \mathbb{Q}^\times$ is a group homomorphism: in other words, show that for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$ we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

d) Show that the restriction of the conjugation map to $\mathbb{Z}[\sqrt{D}]$ is a ring isomorphism $\mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}]$.
e) Show that for $\alpha \in \mathbb{Q}(\sqrt{D})$, we have $N(\alpha) = 0$ iff $\alpha = 0$.
f) Show that for $\alpha \in \mathbb{Z}[\sqrt{D}]$, we have $N(\alpha) \in \{\pm 1\}$ iff $\alpha \in \mathbb{Z}[\sqrt{D}]^\times$ – i.e., iff α has an inverse in the ring $\mathbb{Z}[\sqrt{D}]$.

Exercise 4.1.4. a) Let $x + yi \in \mathbb{Z}[i]$ be such that $N(x + iy) = x^2 + y^2$ is a prime number p. Show that $x + iy$ is irreducible in $\mathbb{Z}[i]$.
b) Let $p \equiv 3 \pmod 4$ be a prime number. Show that p is irreducible *as an element of* $\mathbb{Z}[i]$ even though $N(p) = p^2$ is composite.

Exercise 4.1.5. Find all integers n that are of the form $x^2 - y^2$ for $x, y \in \mathbb{Z}$.

Exercise 4.1.6. Factor $123 + 456i$ in $\mathbb{Z}[i]$.
(Suggestion: begin by factoring its norm. Feel free to ask a computer to do it!)

Exercise 4.1.7. Check carefully that the factorization

$$3 \cdot 7 = 21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

shows that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

5. Homework 5

5.1. **4400 Problems.**

Exercise 5.1.1.
a) Find all $\mathbb{Z}$-solutions – up to scaling – of the equation $3X^2 + 7Y^2 - 3Z^2 = 0$.
b) Can you modify your solution to part a) to give a nice description of all primitive integer solutions?

Exercise 5.1.2. (For D. Petmecky[2]) Show that the equation $3X^2 + 5Y^2 - Z^2 = 0$ has no $\mathbb{Z}$-solutions except $(0, 0, 0)$.

Exercise 5.1.3. Fix $D \in \mathbb{Z}$. We say that $n \in \mathbb{Z}$ is **primitively represented** by the form $x^2 - Dy^2$ if there are **coprime** integers x, y such that $x^2 - Dy^2 = n$. Find all nonzero integers n that are primitively represented by $x^2 + y^2$.

Exercise 5.1.4. Let $D \notin \{0, 1\}$ be a squarefree integer.
a) Show that the units in $\mathbb{Z}[\sqrt{-1}]$ are precisely $\pm 1, \pm\sqrt{-1}$.
b) Show: for all $D \leq -2$, the units in $\mathbb{Z}[\sqrt{D}]$ are precisely ± 1.
c) For each $D \in \{2, 3, 5, 6, 7, 10\}$, prove or disprove that $\mathbb{Z}[\sqrt{D}] = \{\pm 1\}$.

Exercise 5.1.5. $*$ Consider the prime $13 \equiv 1 \pmod 4$. By Fermat's Theorem, it is a sum of 2 squares: $13 = 2^2 + 3^2$. From this representation, we deduce several more representations: also

$$13 = (-2)^2+3^2 = 2^2+(-3)^2 = (-2)^2+(-3)^2 = 3^2+2^2 = (-3)^2+2^2 = 3^2+(-2)^2 = (-3)^2+(-2)^2,$$

thus there are eight representations altogether.
a) Show: any prime $p \equiv 1 \pmod 4$ has precisely 8 representations as a sum of two

[2]Here is an example in which reducing modulo 4 is not sufficient!

squares.
(Suggestion: Consider the prime factorization of p in $\mathbb{Z}[i]$ and use part a) of the previous exercise.)
b) Let $n \in \mathbb{Z}^+$. How many representations does n have as a sum of 2 squares?

Exercise 5.1.6. a) Prove the following algebraic identity: for all $x_1, x_2, y_1, y_2 \in \mathbb{R}$,

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

b) Let $D \in \mathbb{Z}$. Prove the following algebraic identity: for all $x_1, x_2, y_1, y_2 \in \mathbb{R}$,

$$(x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2) = (x_1x_2 - Dy_1y_2)^2 + D(x_1y_2 + x_2y_1)^2.$$

c) When $D \notin \{0, 1\}$ is squarefree, interpret the identity of part b) in terms of the quadratic ring $\mathbb{Z}[\sqrt{D}]$. (Note however that the identity holds for *all* D.)

Exercise 5.1.7. ("No forgiveness")
a) Recall that a positive integer can be uniquely written in the form $n = st^2$ for s squarefree and that s is called the **squarefree part** of n. Show that the Full Two Squares Theorem can be restated as follows: a positive integer is a sum of two square iff its squarefree part is a sum of two squares and a squarefree positive integer is a sum of two squares iff it is not divisible by any prime $p \equiv 3 \pmod 4$.
b) Let m and n be coprime positive integers. Show: if m is not a sum of two squares, then mn is not a sum of two squares.

Exercise 5.1.8. Adapt the proof of the Full Two Squares Theorem to show: a positive integer n is of the form $x^2 + 2y^2$ if and only if $\text{ord}_p(n)$ is even for every prime number p such that -2 is *not* a square modulo p.

Exercise 5.1.9. a) Show that there are $x, y \in \mathbb{Z}$ such that $x^2 - 2y^2 = -1$.[3]
b) Adapt the proof of the Full Two Squares Theorem to show: a nonzero integer n is of the form $x^2 - 2y^2$ if and only if $\text{ord}_p(n)$ is even for every prime number p such that 2 is *not* a square modulo p.

Exercise 5.1.10. a) Show that there are *not* $x, y \in \mathbb{Z}$ such that $x^2 - 3y^2 = -1$.
b) Let $p > 3$ be a prime number such that 3 is a square modulo p. Show: there are $x, y \in \mathbb{Z}$ such that $x^2 - 3y^2 = (-1)^{\frac{p-1}{2}}p$.
(From what we did in class we know that $|x^2 - 3y^2| = p$. So the matter of it is which signs we can take.)
c) $*$ State and prove a precise criterion for when an integer n is of the form $x^2 - 3y^2$.
(Again the trickiest part here is determining the sign conditions on n.)

Exercise 5.1.11. a) Determine exactly which primes $p < 200$ are of the form $x^2 + 3y^2$. Can you find a pattern for these primes?
b) Determine exactly which primes $p < 200$ are of the form $x^2 + 7y^2$. Can you find a pattern for these primes?

Exercise 5.1.12. a) Determine exactly which primes $p < 200$ are of the form $x^2 + 5y^2$. Can you find a pattern for these primes?
b) Show: if $x^2 + 5y^2 = p$ then $p \equiv 1 \pmod 4$.

Exercise 5.1.13. a) Determine exactly which primes $p < 200$ are of the form $x^2 + 14y^2$. Can you find a pattern for these primes?
b) For each of $D \in -3, -5, -7, -14$ and each $N \in \{2, 3, 4, 5, 6\}$ use a computer

[3]Yes, this is easy! But soon enough you should appreciate why we are starting here.

program to count the number of primes $p < 10^N$ that are of the form $x^2 - Dy^2$. Divide by the total number of primes $p < 10^N$ to get a proportion. What do you observe about this proportion for each fixed D as N increases?
c) Perform similar computations to the above for other values of D and/or larger N. What do you observe?

5.2. **6400 Problems.**

Exercise 5.2.1. Let R be an atomic domain. Show that R is a UFD iff every irreducible element of R is prime.

Exercise 5.2.2. Let R be an integral domain with fraction field F. We say that F is **integrally closed in F** if for all $\alpha \in F$, if α satisfies a monic polynomial relation – i.e., $f(\alpha) = 0$ for some $f = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in R[t]$ – then $\alpha \in R$.
a) Please check that we showed in the lectures (and in Chapter 1 of the text) that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.
b) Adapt the proof of this result to show that if R is a UFD then R is integrally closed in F.

Exercise 5.2.3. Let $D \notin \{0, 1\}$ be a squarefree integer.
a) If $D \equiv 1 \pmod 4$, show that the element $\frac{1+\sqrt{D}}{2} \in \mathbb{Q}(\sqrt{D})$ satisfies a monic polynomial with coefficients in $\mathbb{Z}$. Deduce that the ring $\mathbb{Z}[\sqrt{D}]$ is not a UFD.
b) $*$ Show that the ring $\mathbb{Z}[\sqrt{D}]$ is integrally closed in $\mathbb{Q}(\sqrt{D})$ iff $D \equiv 2, 3 \pmod 4$. (Honestly, showing this from scratch is more trouble than it is worth. In the context of a larger discussion of algebraic number theory, it gets a lot easier.)
c) $***$ Prove or disprove: there are infinitely many prime numbers $p \equiv 3 \pmod 4$ such that $\mathbb{Z}[\sqrt{p}]$ is a UFD.

6. Homework 6

6.1. **4400 Problems.**

Exercise 6.1.1. Let m_1, m_2, m, n be positive integers, and let $a \in \mathbb{Z}$.
a) Show: if a is a square modulo n and $m \mid n$ then a is a square modulo m.
b) Show: if $\gcd(m_1, m_2) = 1$ and a is a square modulo both m_1 and m_2, then a is a square modulo $m_1 m_2$.
c) Show: if a is a square modulo both m_1 and m_2 then a is a square modulo $\operatorname{lcm}(m_1, m_2)$.
d) Find m_1, m_2, a such that a is a square modulo m_1 and a is a square modulo m_2 but a is not a square modulo $m_1 m_2$.

Exercise 6.1.2. For each odd prime $p \leq 103$, compute all quadratic residues mod p – i.e., all squares in $\mathbb{Z}/p\mathbb{Z}$.

Exercise 6.1.3. Evaluate these Legendre symbols (the denominators are all prime numbers):

$$\left(\frac{85}{101}\right), \left(\frac{29}{241}\right), \left(\frac{101}{1987}\right), \left(\frac{31706}{43789}\right).$$

Exercise 6.1.4. For the following $a \in \mathbb{Z}$, find all odd primes p such that $\left(\frac{a}{p}\right) = 1$.
a) $a = 169$.
b) $a = 53$.
c) $a = 31$.

d) $a = 21$.
e) $a = 2018$.

Exercise 6.1.5. Use Quadratic Reciprocity to show the following result first stated (but not proved) by Euler: let p and q be distinct odd primes.
a) If $q \equiv 1 \pmod 4$, then $\left(\frac{q}{p}\right) = 1$ iff p is congruent to a square modulo q – hence lies in one of $\frac{q-1}{2}$ residue classes modulo q.
b) If $q \equiv -1 \pmod 4$, then $\left(\frac{q}{p}\right) = 1$ iff $p \equiv \pm x^2 \pmod{4q}$.

Exercise 6.1.6. Show that Quadratic Reciprocity is equivalent to the following statement: for distinct odd primes $p \neq q$, we have

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right).$$

Exercise 6.1.7. Prove the following fact, which we used in the proof of quadratic reciprocity: let $a \in \mathbb{Z}$, let p be an odd prime and let $\zeta_p = e^{2\pi i/p}$ be a primitive pth root of unity. Then

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p & a \equiv 0 \pmod p \\ 0 & a \not\equiv 0 \pmod p \end{cases}.$$

Exercise 6.1.8. ∗∗ Our proof of quadratic reciprocity computes *the square* of the quadratic Gauss sum:

$$\tau^2 = p^* := (-1)^{\frac{p-1}{2}} p.$$

Of course this means that $\tau = \pm\sqrt{p^*}$. Prove that in fact $\tau = \sqrt{p^*}$.

Gauss conjectured that $\tau = \sqrt{p^*}$ in 1801. From then on "seldom a week had passed" in which he did not try to prove his conjecture. He finally succeeded in 1805, writing

Wie der Blitz einschlägt, hat sich das Räthsel gelöst.

This should serve to warn you that this exercise is *very* difficult! However, for one bonus point[4], translate Gauss's quotation into English.

7. Homework 7

7.1. **4400 Problems.**

Heads up: There is an online applet for finding the fundamental solution to a Pell equation, available at

`http://www.numbertheory.org/php/pell.html`

When asked for the fundamental solution u to a Pell equation, you can use this applet, learn about continued fractions and try to find the solution yourself, or do some combination of the two.

[4]Whatever that means!

Exercise 7.1.1. Prove the following Lemma from the text: let (x, y) be a nontrivial solution to $x^2 - Dy^2 = 1$. Then:
(i) We have $x, y, > 0$ iff $x + \sqrt{D}y > 1$.
(ii) We have $x > 0$, $y < 0$ iff $0 < x + \sqrt{D}y < 1$.
(iii) We have $x < 0$, $y > 0$ iff $-1 < x + \sqrt{D}y < 0$.
(iv) We have $x, y < 0$ iff $x + \sqrt{D}y < -1$.

Exercise 7.1.2. Find all integral solutions to the following (Pell) equations:
a) $x^2 - 5y^2 = 1$.
b) $x^2 - 53y^2 = 1$.
c) $x^2 - 73y^2 = 1$.
d) $x^2 - 1006009y^2 = 1$.

Exercise 7.1.3. a) Show: for any positive, nonsquare integer D and any positive integer M there are infinitely many integral solutions to $x^2 - Dy^2 = 1$ with $y \equiv 0 \pmod{M}$. (Suggestion: "change variables" $y = My'$.)
b) Can we always find solutions with $x \equiv 0 \pmod{M}$?

Exercise 7.1.4. A **triangular number** is a positive integer of the form

$$1 + \ldots + m = \frac{m(m+1)}{2}.$$

A **square number** is a number of the form n^2. A **square-triangular number** is a number that is simultaneously triangular and square, i.e., a solution to

$$\frac{m(m+1)}{2} = n^2.$$

a) Show that the above equation simplifies to

$$8n^2 = (2m+1)^2 - 1.$$

b) Substitute $x = 2m+1$, $y = 2n$ and show that solutions to $x^2 - 2y^2 = 1$ correspond to square-triangular numbers, via

$$m = \frac{x-1}{2}, \ n = \frac{y}{2}.$$

c) Use this correspondence to find all square-triangular numbers.

Exercise 7.1.5. Let D be a positive, nonsquare integer. The **negative Pell equation** is

$$x^2 - Dy^2 = -1.$$

When D is not a square, integral solutions correspond to units of norm -1 in $\mathbb{Z}[\sqrt{D}]$. However, the issue of whether such units exist is much more complicated than for the Pell equation itself.
a) Find all solutions to the negative Pell equation when D is a square.
b) Suppose that D is a square and that the negative Pell equation has an integral solution. Show: D is not divisible by 4 and that D is not divisible by any prime $p \equiv 3 \pmod{4}$.
c)$*$ Find a nonsquare value of D satisfying all the necessary conditions of part b) but for which the negative Pell equation nevertheless has no solutions.

Remark 1. *It can be shown that (for nonsquare D) the negative Pell equation $x^2 - Dy^2 = -1$ has solutions iff the period length of the continued fraction expansion of $\sqrt{D}$ is even. However this condition is arguably a bit awkward: it does not say*

much about the set of D's for which there is a solution, and for a given D, the amount of computation necessary to check this condition can be considerable.

Exercise 7.1.6. For D a positive, nonsquare integer and N a nonzero integer, one can consider the **generalized Pell equation**

$$x^2 - Dy^2 = N.$$

Suppose that this equation has a $(+,+)$ solution – i.e., a solution in positive integers x, y. Show: it has infinitely many $(+,+)$ solutions.

Exercise 7.1.7. Let $a, k \geq 2$ be integers. Suppose that $a^k - 1$ is prime. Show: $a = 2$ and k is prime.

Exercise 7.1.8. It is a result of Euler that if n is any even perfect number, then n is of the form $2^{k-1}(2^k - 1)$ for a prime number $2^k - 1$. (By the previous exercise, this implies that k is also prime.) In this exercise you will fill in the details of a proof. Since n is even, we may write $n = 2^{k-1}m$ with $k \geq 2$ and m odd.
a) Show:

$$2^k m = 2n = \sigma(n) = (2^k - 1)\sigma(m). \tag{1}$$

b) Deduce from (1) that $2^k - 1 \mid m$ and thus there is $M \in \mathbb{Z}$ such that $m = (2^k - 1)M$.
c) Deduce from (1) that

$$2^k M = \sigma(m). \tag{2}$$

d) Explain why

$$\sigma(m) \geq m + M = 2^k M = \sigma(m),$$

and deduce that

$$\sigma(m) = m + M. \tag{3}$$

e) Deduce from (3) that m is prime and $M = 1$.
f) Complete the proof.

7.2. **6400 Problems.**

Exercise 7.2.1. Let D be a positive nonsquare integer. Show tha tthe unit group $\mathbb{Z}[\sqrt{D}]^\times$ of the ring $\mathbb{Z}[\sqrt{D}]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. (Comment: this is true whether or not there is a solution to the negative Pell equation, but the isomorphism works a bit differently in the two cases.)

8. Homework 8

8.1. **4400 Problems.**

Exercise 8.1.1. Show that for all $n \geq 2$ we have $\varphi(n) \leq n - 1$, with equality if and only if n is prime.

Exercise 8.1.2. Show that $\varphi(n)$ is even for all $n \geq 2$.

Exercise 8.1.3. Show that there are infinitely many integers n such that $\varphi(n) \equiv 0 \pmod 4$ and infinitely many integers n such that $\varphi(n) \equiv 2 \pmod 4$.
(You may use Dirichlet's theorem on primes in arithmetic progressions.)

Exercise 8.1.4. Fill in the details of the proof of the following claim: $\varphi(n) \geq \sqrt{\frac{n}{2}}$.
a) Write $n = p_1^{a_1} \cdots p_r^{a_r}$ be the standard form factorization. Show that

$$\frac{\varphi(n)^2}{n} = \prod_{i=1}^{r} p_i^{a_i - 2}(p_i - 1)^2 \geq \prod_{i=1}^{r} \frac{(p_i - 1)^2}{p_i}.$$

b) Suppose $p \geq 3$. Show that $\frac{(p-1)^2}{p} \geq 1$.
c) Show that if n is odd then $\frac{\varphi(n)^2}{n} \geq 1$, whereas if n is even then $\frac{\varphi(n)^2}{n} \geq \frac{(2-1)^2}{2} = \frac{1}{2}$, and deduce the result.

Exercise 8.1.5. a) Use the previous exercise to show that $\lim_{n\to\infty} \varphi(n) = \infty$.
b) Give an independent proof that $\lim_{n\to\infty} \varphi(n) = \infty$.
c) Deduce: for all $N \in \mathbb{Z}^+$, the set $\{n \in \mathbb{Z}^+ \mid \varphi(n) = N\}$ is finite.

Exercise 8.1.6. Let $n \in \mathbb{Z}^+$.
a) Show: $\varphi(n) = 1 \iff n \in \{1, 2\}$.
b) Show: $\varphi(n) = 2 \iff n \in \{3, 4, 6\}$.
c) Find all $n \in \mathbb{Z}^+$ such that $\varphi(n) = 4$.

Exercise 8.1.7. Calculate $\Phi_{105}(X)$.
(Suggestion: use the formula in §8.4.2 of the text – also derived in class – together with a computer algebra system to perform the multiplication and division.)

Exercise 8.1.8. Investigate the literature on coefficients of cyclotomic polynomials and report on what you find.

8.2. **6400 Problems.**

Exercise 8.2.1. Prove the following analogue of the Prime Number Theorem: fix a prime number p. For $n \in \mathbb{Z}^+$, let $I(p, n)$ be the number of monic irreducible polynomials $f \in \mathbb{Z}/p\mathbb{Z}[X]$ of degree n. Show that as $n \to \infty$ we have

$$I(p, n) \sim \frac{p^n}{n},$$

i.e.,

$$\lim_{n\to\infty} \frac{I(p, n)}{p^n/n} = 1.$$

(Suggestion: use the formula for $I(p, n)$ of Theorem 8.24 of the course text. Use the fact that a proper divisor of n is at most $\frac{n}{2}$.)

Exercise 8.2.2. Investigate the connections between Möbius Inversion and the Principle of Inclusion-Exclusion.
(One deep connection is via a more general notion of a Möbius function of a suitable partially ordered set. For a well written introduction, see
`http://alpha.math.uga.edu/~pete/Bender-Goldman75.pdf`

9. Homework 9

9.1. **4400 Problems.**

Exercise 9.1.1. Write out a careful proof of the following fact mentioned in class: let $N \in \mathbb{Z}^+$. Given any sequence $a_1, \ldots, a_N \in \mathbb{Z}$, there are $1 \leq i \leq j \leq N$ such that $a_i + a_{i+1} + \ldots + a_j \equiv 0 \pmod{N}$.

Exercise 9.1.2. For $r > 0$, let

$$L(r) := \#\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 \leq r^2\}$$

be the number of lattice points lying on or inside the closed disk of radius r centered at 0.
a) Explain why $\lim_{r\to\infty} \frac{L(r)}{r^2} = \pi$.
b) Compute $L(10)/10^2$ and compare to π.
c) Write a computer program to compute $L(10^k)/10^{2k}$ and compare to π for several values of k. How many decimal places of accuracy can you get?

Exercise 9.1.3. Read about the Gauss Circle Problem and write a brief statement about it. What is the best currently known result?

Exercise 9.1.4. Here is a Lemma from the textbook: for a prime $p > 2$ and $a \in \mathbb{Z}$, there are $r, s \in \mathbb{Z}$ such that $r^2 + s^2 \equiv a \pmod{p}$. The textbook proves this using an elementary counting argument. Deduce this from the Chevalley-Warning Theorem applied to the polynomial $x^2 + y^2 - az^2$.

Exercise 9.1.5. $*$ Let $\Omega \subset \mathbb{R}^N$ be a convex body that is moreover *closed* (equivalently, compact). Show: if $\mathrm{Vol}(\Omega) = 2^N$, then $\Omega \cap \mathbb{Z}^N \supsetneq \{0\}$, i.e., Ω has a nonzero lattice point.
(Hint: the hypotheses ensure that for all $\epsilon > 0$, the dilate $(1+\epsilon)\Omega$ has a nonzero lattice point.)

Exercise 9.1.6. Let P be a simple lattice polygon. (That is, P is a simple closed polygonal curve.) Show that P can be dissected as a finite union of lattice triangles.

Exercise 9.1.7. The Gauss-Legendre Three Squares Theorem states that a positive integer n is a sum of three integral squares *unless* n is of the form $4^a(8k+7)$. Deduce the Four Squares Theorem from the Three Squares Theorem.

Exercise 9.1.8. a) Prove Euler's Identity: For any integers $a_1, \ldots, a_4, b_1, \ldots, b_4$, we have

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 +$$
$$(a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.$$

b) Deduce from Euler's Identity, that for any ring R, if $x, y \in R$ are both sums of four squares in R, then so is xy.
c) Find $a, b \in \mathbb{Z}$ such that a and b are each sums of three squares but ab is not.

Exercise 9.1.9. Identify and state the following theorems about quadratic forms:
a) The Conway-Schneeberger 15 Theorem.
b) The Bhargava-Hanke 290 Theorem.
c) The Rouse 451 Theorem.

Exercise 9.1.10. For each of the following (isotropic binary) quadratic forms, find all integers it represents.
a) $x^2 + 2xy$.
b) $x^2 + 3xy$.
c) $x^2 + 4xy$.
d) $2x^2 + 5xy$.
e) Why did we *not* ask about $x^2 + 5xy$?