CS 103X: Discrete Structures
Homework Assignment 3 — Solutions

Exercise 1 (20 points)**.** On well-ordering and induction:

(a) Prove the induction principle from the well-ordering principle.

(b) Prove the well-ordering principle from the induction principle.

Conclude that the principles of induction, strong induction, and well-ordering are equally powerful.

Solution

(a) Consider the premises of induction - a set A of positive integers exists such that $1 \in A$ and, if $n \in A$ then $(n+1) \in A$ for any $n \in \mathbb{N}^+$. Consider the set $B = \mathbb{N}^+ \setminus A$, the set of all positive integers not in A. Assume for the sake of contradiction that B is nonempty. By the well ordering principle, B must have a least element. We know that $1 \notin B$ because one of the induction premises is $0 \in A$. Thus there is some least element $b \in B$ with $b > 1$, which implies $b - 1 \in A$. But then from the second induction premise, $b = (b-1) + 1 \in A$, which contradicts the earlier assertion that $b \notin A$. Thus the assumption that B is nonempty is incorrect, so $B = \emptyset$ and $A = \mathbb{N}^+$. Thus, assuming the well-ordering principle, if the premises of induction hold for a set A then $A = \mathbb{N}^+$, which proves the induction principle.

(b) Recall that in the last homework, we proved that strong induction follows from the induction principle, so proving well-ordering from strong induction will suffice. Again we proceed by contradiction; assume there is a nonempty set A of positive integers without a least element. We will use strong induction to show that this cannot be. Since 1 is the smallest positive integer, $1 \notin A$ since it would be the least element. Assume that the positive integers from 1 to k are not in A. Then if $(k+1) \in A$, $(k+1)$ would be the smallest element so $(k+1) \notin A$. Then by strong induction all positive integers are not in A, so $A = \emptyset$, a contradiction. Therefore the assumption was incorrect and any nonempty set of positive integers must have a least element. Thus the well-ordering principle holds if the induction principle holds.

To conclude, since each principle can be proved from the other, any problem solvable with one can also be solved by the other. Thus the well-ordering principle, induction principle, and the induction principle are equally powerful.

Exercise 2 (20 points)**.** (a) Let's develop another proof that $\sqrt{2}$ is irrational. Assume as we did in class that there exist two numbers $p, q \in \mathbb{Z}$, with $q \neq 0$, such that

$$\frac{p}{q} = \sqrt{2}.$$

Show that

$$\frac{2q-p}{p-q} = \sqrt{2}.$$

Use the well-ordering principle to complete the argument, and write the whole proof formally.

(b) Use the Fundamental Theorem of Arithmetic to prove that for $n \in \mathbb{N}$, $\sqrt{n}$ is irrational unless n is a perfect square, that is, unless there exists $a \in \mathbb{N}$ for which $n = a^2$.

Solution

(a) From $\frac{p}{q} = \sqrt{2}$, square both sides and multiply by q^2 to get $p^2 = 2q^2$. Subtract pq from both sides to get $p^2 - pq = 2q^2 - pq$, which can be factored as

$$p(p-q) = q(2q-p).$$

This can be rearranged to

$$\frac{p}{q} = \frac{2q-p}{p-q}$$

(Note that this requires dividing by both q and $(p-q)$, so neither of these can be 0. $q \neq 0$ was one of our initial assumptions, and since $\frac{p}{q} = \sqrt{2}$, $p \neq q$ and $p - q \neq 0$.) Since $\frac{p}{q} = \sqrt{2}$,

$$\frac{2q-p}{p-q} = \sqrt{2}.$$

Since $\sqrt{2} > 0$, we can claim that if integers p, q exist with $q \neq 0$ and $\frac{p}{q} = \sqrt{2}$, natural numbers m, n must exist with the same properties — p and q must have the same sign so we can set $m = |p|$ and $n = |q|$. Let A be the set of all such $n \in \mathbb{N}$. By the well-ordering principle, A must have a least element, so let n' be the least element, and m' the corresponding natural number such that $\frac{m'}{n'} = \sqrt{2}$. But from the first paragraph, $\frac{2n'-m'}{m'-n'} = \sqrt{2}$ and thus $(m'-n') \in A$. Since $\sqrt{2} < 2$, $m' < 2n'$ so $(m'-n') < 2n'-n'$ or $(m'-n') < n'$. This contradicts the fact that n' was the least element of A, so our initial assumption that $\sqrt{2}$ is rational is incorrect. This completes the proof.

(b) We will prove the statement by contradiction. Assume $n \in \mathbb{N}$ is not a perfect square, yet its square root is a rational number $\frac{p}{q}$ for coprime integers p, q, where $q \neq 0$. So $\sqrt{n} = \frac{p}{q}$ or $n = \frac{p^2}{q^2}$. Without loss of generality, we can assume both p and q are non-negative. If $p = 0$, then $n = 0$ which is a perfect square, contradicting our assumption. So we can assume both p and q are positive. By the Fundamental Theorem of Arithmetic, we can uniquely write both p and q as products of primes, say $p = p_1 p_2 \dots p_m$ and $q = q_1 q_2 \dots q_n$. Since p and q are coprime, they have no common factors, so $p_i \neq q_j$ for all $1 \leq i \leq m$, $1 \leq j \leq n$. We have:

$$p^2 = (p_1 p_2 \dots p_m)^2 = p_1^2 p_2^2 \dots p_m^2$$

and

$$q^2 = (q_1 q_2 \dots q_n)^2 = q_1^2 q_2^2 \dots q_n^2$$

Now p^2 and q^2 cannot have any common factors > 1 — if they did have a common factor $d > 1$, any prime factor f of d (and there must be at least one such) must also be a common prime factor of p^2 and q^2 (transitivity of divisibility). By the Fundamental Theorem of Arithmetic, $p_1^2 p_2^2 \dots p_m^2$ is the unique prime factorization of p, so f must be one of the primes $p_1, p_2, \dots, p_m$. Similarly, f must also be one of the primes $q_1, q_2, \dots, q_n$. But this contradicts our statement that no $p_i = q_j$. So p^2 and q^2 are coprime.

A ratio of natural numbers in lowest terms is itself a natural number if and only if its denominator is 1. Since $n \in \mathbb{N}$, we must have $q^2 = 1$, which implies $q = 1$. But then n must be the perfect square p^2, which contradicts our assumption.

The statement is thus proved by contradiction.

Exercise 3 (20 points)**.** Prove or disprove, for integers a, b, c and d:

(a) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

(c) If a and b are perfect squares and $a \mid b$, then $\sqrt{a} \mid \sqrt{b}$.

(d) If $ab \mid cd$, then $a \mid c$ or $a \mid d$.

Solution

(a) If $a \mid b$ then $b = ma$ for some integer m and if $a \mid c$ then $c = na$ for some integer n. Thus $(b + c) = ma + na = (m + n)a$. Since $m + n$ is an integer, $a \mid (b + c)$.

(b) The proof is essentially identical to that of Theorem 5.1.1.a. Since $\gcd(a, b) = 1$, there exist integers u, v with $au + bv = 1$. Multiply both sides by c to get $c = auc + bcv$ (by the result of the first part of this exercise). We know that $a \mid bc$ so $a \mid bcv$ and of course $a \mid auc$, so $a \mid (auc + bcv)$. Thus $a \mid c$.

(c) Proof by contradiction: Assume $\sqrt{b}$ is not divisible by $\sqrt{a}$. Consider the prime factorizations of $\sqrt{a}$ and $\sqrt{b}$ - there must be some prime p that appears m times in the prime factorization of $\sqrt{a}$ and n times in the prime factorization of $\sqrt{b}$ with $m > n$. The prime factorizations of perfect squares include every element of their square root's factorization twice, so p must occur $2m$ times in the prime factorization of a and $2n$ times in the prime factorization of b. But $2m > 2n$, which implies that b is not divisible by a, a contradiction. Therefore $\sqrt{a} \mid \sqrt{b}$.

(d) False. One possible counterexample is $a = 10, b = 1, c = 4, d = 25$.

Exercise 4 (25 points)**.** On Euclid's algorithm:

(a) Write the algorithm in pseudo-code. (10 points)

(b) State a theorem that asserts the correctness of the algorithm and prove the theorem. (10 points)

(c) Use the algorithm to calculate gcd(5924, 6892). Write out the complete sequence of derivations. (5 points)

Solution

(a) Procedure `GCD-Euclid`
Input: Integers a, b, not both 0.

i. $a = |a|$, $b = |b|$ (These three lines are needed only for the
ii. If $b > a$ then swap a and b first recursive call and can be factored out
iii. If $b = 0$, then return a with a second procedure.)
iv. $q = \lfloor a/b \rfloor$ (Quotient)
v. $r = a - q * b$ (Remainder)
vi. If $r = 0$, then return b
vii. Return `GCD-Euclid`(b, r)

The following nonrecursive version also works:

Procedure `GCD-Euclid-Nonrecursive`
Input: Integers a, b, not both 0.

i. $a = |a|$, $b = |b|$
ii. If $b > a$ then swap a and b
iii. If $b = 0$, then return a
iv. Do
v. $q = \lfloor a/b \rfloor$ (Quotient)
vi. $r = a - q * b$ (Remainder)
vii. If $r = 0$, then return b
viii. $a = b$
ix. $b = r$
x. Loop

(b) **Theorem.** Euclid's Algorithm correctly finds the GCD of a and b in a finite number of steps.

Proof. We will prove the correctness of the algorithm in the context of the recursive listing above. The proof for the non-recursive version is identical except that it is slightly more difficult to phrase correctly. The first couple of lemmas help to justify the assumption $a > b > 0$ in the lecture notes.

Lemma 1. $d \mid a$ if and only if $d \mid |a|$.

Proof. First we show that if $d \mid x$, then $d \mid -x$. By the Division Algorithm, $x = qd$ for some integer q, so $-x = -qd = (-q)d$. Since $-q$ is obviously integral if q is (and the Division Algorithm guarantees that this is an unique representation given x, d), d divides $-x$.

So if $d \mid a$, then $|a|$ is either a, which is trivially divisible by d, or $-a$, which by the above reasoning is also divisible by d. Similarly, if $d \mid |a|$, then a is either $|a|$ or $-|a|$, both of which are divisible by d as above. This proves the result. □

Lemma 2. $\gcd(a, b) = \gcd(|a|, |b|) = \gcd(|b|, |a|)$

Proof. Let $d = \gcd(a, b)$. Since $d = \gcd(a, b)$, $d \mid a$ and $d \mid b$, so by Lemma 1, $d \mid |a|$ and $d \mid |b|$, i.e. d is a common divisor of $|a|$ and $|b|$. Now we prove by contradiction that d is the greatest such divisor. Assume there is some $c > d$ such that $c \mid |a|$ and $c \mid |b|$. Then by Lemma 1, $c \mid a$ and $c \mid b$. So c is a common divisor of a and b strictly greater than the GCD of a and b, which contradicts the definition of the GCD. Therefore we must have $\gcd(a, b) = \gcd(|a|, |b|)$.

Also, the definition of $\gcd(x, y)$ is clearly symmetric in x and y, so $\gcd(|a|, |b|) = \gcd(|b|, |a|)$. Hence proved. □

Let $P(n)$ be the following statement:

> "Euclid's Algorithm finds the correct GCD of a and b in a finite number of steps, for all $0 \leq a, b \leq n$ (a and b not both 0)."

We will prove $P(n)$ holds for all positive integers n by induction. We assume $a \geq b$: if not, the first couple of steps of the algorithm will take their absolute values and swap them if necessary so the relation holds, and by Lemma 2 the GCD of these two new values is precisely the same as the GCD of the original values. The base case, $n = 1$, has two possibilities: $a = 1$, $b = 0$, or $a = 1, b = 1$. In the first case, the third line of the algorithm returns the correct GCD 1, and in the second case r evaluates to 0 before any recursive calls, so the correct GCD $b = 1$ is returned, in a finite number of steps (no recursive calls, so at most 6 lines of pseudocode).

Now assume $P(n)$ is true and consider $P(n + 1)$, where we allow the values of a and b to be at most $n + 1$. If $b = 0$, the third line returns the correct GCD, a. If $b \mid a$, $\gcd(a, b) = b$, which is the value returned by the algorithm since r evaluates to 0. Otherwise, the algorithm recursively computes and returns $\gcd(b, r)$. Now by Lemma 4.3.1 in the lecture notes, $\gcd(a, b) = \gcd(b, r)$. Also, since $0 \leq r < b \leq n + 1$, r and b are both at most n (if b was $n+1$, a would also be $n+1$, which implies $b \mid a$, which is a

case we have already handled) and not both zero. Hence by the inductive hypothesis, Euclid's Algorithm correctly computes $\gcd(b, r)$ in a finite number of steps, which implies that it also correctly computes $\gcd(a, b)$ in a finite number of steps, since the sequence of steps before the recursive call adds only a finite overhead. Hence $P(n+1)$ is true. This proves the claim by induction. The truth of $P(n)$ for all $n \in N^+$ obviously implies the theorem. □

(c) The first step of the algorithm swaps 5924 and 6892 so $a = 6892$, $b = 5924$. We tabulate the values of a, b and r in each successive iteration until $r = 0$:

Iteration	a	b	r
1	6892	5924	968
2	5924	968	116
3	968	116	40
4	116	40	36
5	40	36	4
6	36	4	0

The value of b when r is zero is 4, so this is the GCD.

Exercise 5 (15 points)**.** Some prime facts:

(a) Prove that for every positive integer n, there exist at least n consecutive composite numbers. (10 points)

(b) Prove that if an integer $n \geq 2$ is such that there is no prime $p \leq \sqrt{n}$ that divides n, then n is a prime. (5 points)

Solution

(a) Recall the definition $n! = 1 \times 2 \times 3 \times \cdots \times n$ for any positive integer n. Consider the consecutive positive integers $(n+1)! + 2, (n+1)! + 3, ...(n+1)! + (n+1)$. By definition of factorial, all integers from 2 to $(n+1)$ divide $(n+1)!$, so $2 \mid ((n+1)!+2)$, $3 \mid ((n+1)!+3)$, and so on up to $(n+1) \mid ((n+1)!+(n+1))$ (remember the property of divisibility proved in Exercise 3a.) Thus all members of this sequence are composite, making n consecutive composite numbers. This sequence can be generated for any n, so for all n there exists at least n consecutive composite numbers.

(b) Proof by contradiction: Assume n is not prime. By Theorem 5.1.2, $n = p_1 p_2 ... p_k$ for primes $p_1 \leq p_2 \leq .... \leq p_k$, and since n is not prime $k \geq 2$. Since no prime less than or equal to $\sqrt{n}$ divides n, $\sqrt{n} < p_1 \leq p_2$. Then $p_1 p_2 > n$, so $n = p_1 p_2 ... p_k > n$, a contradiction. Thus our assumption was false and n must be prime.