# CS103X: Discrete Structures
# Homework Assignment 2: Solutions

Due February 1, 2008

**Exercise 1** (10 Points). Prove or give a counterexample for the following:

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:** 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 $n = (\frac{p}{q})^2$. 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 $p = p_1 p_2 \ldots p_m$ and $q = q_1 q_2 \ldots q_n$. 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:

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

and

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

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, $p_1^2 p_2^2 \ldots p_m^2$ is the unique prime factorization of $p$, so $f$ must be one of the primes $p_1, p_2, \ldots, p_m$. Similarly, $f$ must also be one of the primes $q_1, q_2, \ldots, q_n$. 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 $n \in N$, 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 2** (20 Points). Prove or disprove, for integers $a, b, c$ and $d$:

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

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

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

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

**Solution:**

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

(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 $a|bc$ so $a|bcv$ and of course $a|auc$, so $a|(auc + bcv)$. Thus $a|c$.

(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 roots 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 $\sqrt{a}|\sqrt{b}$.

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

**Exercise 3** (25 Points). On Euclids algorithm:

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

(b) Prove that Euclids Algorithm correctly finds the GCD of $a$ and $b$ in a finite number of steps. (10 points)

(c) Use the algorithm to calculate gcd(1247, 899). Write out the complete sequence of derivations. (5 points)

**Solution:**

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

  i. $a = |a|$, $b = |b|$
  ii. If $b > a$ then swap $a$ and $b$ first
  iii. If $b = 0$, then return $a$
  iv. $q = ba/bc$ (Quotient)
  v. $r = a - q * b$ (Remainder)
  vi. If $r = 0$, then return $b$
  vii. Return `GCD-Euclid`(b, r)

The first three lines are needed only for the recursive call and can be factored out with a second procedure.
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. $q = ba/bc$ (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.** $d|a$ if and only if $d \mid |a|$.
*Proof.* First we show that if $d|x$, then $d| - x$. By the Division Algorithm, $x = qd$ for some integer $q$, so $-x = -qd = (-q)d$. Since $-q$ is obviously integral since $q$ is (and the Division Algorithm guarantees that this is an unique representation given $x$, $d$), $d$ divides $-x$. So if $d|a$, 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 $d = \gcd(a, b)$, $d|a$ and $d|b$, 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, $c|a$ and $c|b$. 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.

Back to the original problem. Let $P(n)$ be the following statement:
"Euclids 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 $b|a$, $\gcd(a, b) = b$, 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 $b|a$, which is a case we have already handled) and not both zero. Hence by the inductive hypothesis, Euclids 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 $n \in \mathbb{N}^+$ obviously implies the theorem.

(c) The first step of the algorithm swaps 1247 and 899 so $a = 1247$, $b = 899$. We tabulate the values of $a$, $b$ and $r$ in each successive iteration until $r = 0$:

| Iteration | a | b | r |
|---|---|---|---|
| 1 | 1247 | 899 | 348 |
| 2 | 899 | 348 | 203 |
| 3 | 348 | 203 | 145 |
| 4 | 203 | 145 | 58 |
| 5 | 145 | 58 | 29 |

The value of $b$ when $r$ is zero is 29, so this is the GCD.

**Exercise 4** (20 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. (10 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 $(n+1)!+2$, $(n+1)!+3$, $\ldots (n+1)!+(n+1)$. By definition of factorial, all integers from 2 to $(n+1)$ divide $(n+1)!$, so $2|((n+1)!+2)$, $3|((n+1)!+3)$, and so on up to $(n+1)|((n+1)!+(n+1))$ (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, $n = p_1 p_2 \ldots p_k$ for primes $p_1 \leq p_2 \leq \ldots \leq p_k$, 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 $n = p_1 p_2 \ldots p_k > n$, a contradiction. Thus our assumption was false and $n$ must be prime.

**Exercise 5** (25 Points) A fun game:

To start with, there is a chart with numbers 1211 and 1729 written on it. Now you and I take turns and you go first. On each players turn, he or she must write a new positive integer on the board that is the difference of two numbers that are already there. The first person who cannot create a new number loses the game.
For example, your first move must be $1729 - 1211 = 518$. Then I could play either $1211 - 518 = 693$ or $1729 - 518 = 1211$, and so forth.

(a) Prove every number written on the chart is a multiple of 7 less than or equal to 1729. (10 points)

(b) Prove that every positive multiple of 7 less than or equal to 1729 is on the chart at the end of the game. (10 points)

(c) Can you predict the winner? What if I go first? (5 points)

**Solution.**

(a) We use induction. Let P(n) be the proposition that after $n$ moves, every number on the board is a positive linear combination of 1729 and 1211.

Base case. P(0) is true because 1729 and 1211 are trivial linear combinations of 1729 and 1211.

Inductive step. Assume that after $n$ moves, every number on the board is a positive linear combination of 1729 and 1211. The next number written on the board is also a positive linear combination, because:

- The rules require the number to be positive.
- The new number must be a difference of two numbers already on the board, which are themselves linear combinations of 1729 and 1211 by assumption. And a difference of linear combinations is another linear combination: difference of linear combinations of x and y can be expressed as $a_1x + b1y - a_2x + b_2y = (a_1 - a_2)x + (b1 - b_2)y$ which is again, a linear combination.

By induction, every number on the board is a positive linear combination of 1729 and 1211. And every positive linear combination of 1729 and 1211 is a multiple of gcd(1729,1211)=7.

(b) Let $x$ be the smallest number on the board at the end of the game. By the Division Algorithm, there exist integers $q$ and $r$ such that $1729 = q \cdot x + r$ where $0 \leq r < x$. When no more moves are possible, $1729 - x$ must already be on the board, and thus so must $1729 - 2x, \ldots, 1729 - (q-1)x$. However, $1729 - qx = r$ can not be on the board, since $r < x$ and $x$ is defined to be the smallest number there. The only explanation is that $r = 0$, which implies that $x|1729$. By a symmmetric argument, $x|1211$. Therefore, $x$ is a common divisor of 1729 and 1211. The only common divisors of 1729 and 1211 are 1 and 7, and $x$ can not be 1 by the preceding part (a). Therefore, 7 is on the board at the end of the game. Since no more moves are possible, $1729 - 7, 1729 - 2 \times 7, \ldots, 7, 0$ must all be on the board as well. So every positive multiple of of 7 less than or equal to 1729 is on the board at the end of the game.

(c) There are $1729/7 = 247$ numbers on the board at the end of the game. Thus, there were $247 - 2 = 245$ moves. First player gets the last move, so whoever goes first wins.