MATH 2112/CSCI 2112, Discrete Structures I
Winter 2007
Toby Kenney
Homework Sheet 6
Hints & Model Solutions

Sheet 5

3 *(b) Prove that there are infinitely many prime numbers congruent to 3 modulo 4.*

Proof. Suppose there are only finitely many primes of this form. Let them be $p_1, p_2, \ldots, p_k$. Now consider $p_1 p_2 \cdots p_k$. If k is even then this is congruent to 1 modulo 4, in which case $p_1 p_2 \cdots p_k + 2 \equiv 3 \pmod{4}$. Therefore, $p_1 p_2 \cdots p_k + 2$ has a prime factor congruent to 3 modulo 4. This can't be any of $p_1, p_2, \ldots, p_k$, so it contradicts the assumption that $p_1, p_2, \ldots, p_k$ were the only such primes.

On the other hand, if k is odd then $p_1 p_2 \cdots p_k$ is congruent to 3 modulo 4, in which case $p_1 p_2 \cdots p_k + 4 \equiv 3 \pmod{4}$. Therefore, $p_1 p_2 \cdots p_k + 4$ has a prime factor congruent to 3 modulo 4. This can't be any of $p_1, p_2, \ldots, p_k$, so it contradicts the assumption that $p_1, p_2, \ldots, p_k$ were the only such primes.

Therefore, in either case, $p_1, p_2, \ldots, p_k$ are not the only such primes, so there must be infinitely many. □

6 *Observe that* $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\left(\sqrt{2}\times\sqrt{2}\right)} = \sqrt{2}^{2} = 2$. *Prove that there are two irrational numbers* α *and* β *such that* α^β *is rational.*

Proof. Either $\sqrt{2}^{\sqrt{2}}$ is rational or it is irrational. In the first case, we can set $\alpha = \sqrt{2}$ and $\beta = \sqrt{2}$, then α and β are irrational, but α^β is rational. On the other hand, if $\sqrt{2}^{\sqrt{2}}$ is irrational, then setting $\alpha = \sqrt{2}^{\sqrt{2}}$ and $\beta = \sqrt{2}$ gives a pair of numbers such that α and β are irrational but α^β is rational. □

Sheet 6

1 *Show that if* $m > 1$ *and* $n > 1$ *are natural numbers such that* $6|mn$*, then it is possible to cover an* $m \times n$ *chessboard with* 3×2 *tiles. [Hint: if* $3|m$ *and* $2|n$*, or* $2|m$ *and* $3|n$*, this should be easy. If* $6|m$ *and* $n > 2$*, divide*

into two cases: $n = 2k + 3$ and $n = 2k$. Prove each of these by induction on k.]

Proof. If $m = 2k$ and $n = 3l$, then we can cover the $m \times n$ chessboard with a k by l block of 3×2 tiles. Similarly if $m = 3k$, and $n = 2l$. On the other hand, if $m = 6k$, we can cover an $m \times 2$ chessboard by putting $2k$ 3×2 tiles in a row, Therefore, if we can cover an $m \times n$ chessboard, then we can cover an $m \times (n + 2)$ chessboard, by just placing our covering of the $m \times 2$ chessboard next to our covering of the $m \times n$ chessboard. Thus, we can cover all $m \times 2l$ chessboards.

We can also cover an $m \times 3$ chessboard by placing $3k$ tiles side by side. Therefore, using the same induction step as before, we can cover all $m \times (3 + 2l)$ chessboards. □

2 *Consider the set of ordered pairs (m, n) of natural numbers, ordered by $(k, l) < (m, n)$ if either $k < m$ or ($k = m$ and $l < n$). [This is called the lexicographic order; it is the way words are ordered in the dictionary.] For example, $(1, 7) < (2, 1)$, and $(3, 4) < (3, 5)$. Show that this set is a well-order.*

Proof. Let A be any non-empty subset of this set. We need to show that A has a smallest element. We consider the set of natural numbers m, for which there is an n such that $(m, n) \in A$. This is a non-empty subset of the natural numbers, so it has a least element m_0 because the natural numbers are a well-order.

Now we consider the set of natural numbers n such that $(m_0, n) \in A$. This is a non-empty subset of the natural numbers, so it has a least element n_0. We will show that (m_0, n_0) is the least element of A. Given any element (k, l) of A, we know that there is an n with $(k, n) \in A$, since $n = l$ works. Therefore, since m_0 was the smallest natural number with this property, we must have $m_0 \leqslant k$. If $m_0 < k$, then by definition of the order on our set, $(m_0, n_0) < (k, l)$. On the other hand, if $m_0 = k$ then $(m_0, l) \in A$, so by definition of n_0, we must have $n_0 \leqslant l$. Thus $(m_0, n_0) < (k, l)$. Since (k, l) was an arbitrary element of A, (m_0, n_0) must be the smallest element of A, so A has a smallest element. □

3 *Show that $\sum_{i=1}^{n} i^2(i + 1) = \frac{n(n+1)(n+2)(3n+1)}{12}$.*

Proof. Induction on n. When $n = 0$ the result obviously holds. Suppose the formula works for some value of n. We want the show that it works for $n + 1$, i.e. that $\sum_{i=1}^{n+1} = \frac{(n+1)(n+2)(n+3)(3(n+1)+1)}{12}$. But $\sum_{i=0}^{n+1} i^2(i + 1) = \sum_{i=0}^{n} i^2(i + 1) + (n + 1)^2(n + 2) = \frac{n(n+1)(n+2)(3n+1)}{12} + (n + 1)^2(n + 2) = (n + 1)(n + 2)\left(\frac{n(3n+1)+12(n+1)}{12}\right) = (n + 1)(n + 2)\frac{3n^2+13n+12}{12} = \frac{(n+1)(n+2)(n+3)(3n+4)}{12}$, so the formula works for $n + 1$. □

4 What is wrong with the following proof that all maths lecturers are the same age?

The problem with the proof given is that when $n = 1$, the induction step doesn't work, because the set $l_2, \ldots, l_n$ is empty, so the fact that $l_2, \ldots, l_n$ have ages both a_1 and a_2 is vacuously true, and does not imply that $a_1 = a_2$.

5 Prove that if $m, n < 2^k$ then Euclid's algorithm finds the greastest common divisor of m and n in at most $2k$ steps.

Proof. Induction on k. If $k = 1$, then m and n have to both be 1, so Euclid's algorithm finishes in just one step.

Now suppose that we know that if $m, n < 2^{k-1}$, then Euclid's algorithm finds the greatest common divisor in at most $2(k-1)$ steps. Without loss of generality, suppose $n < m$. The first step of Euclid's algorithm is to find q and r such that $m = nq + r$, where $r < n$. We also know that $r \leqslant m - n$. Therefore, $2r < n + m - n = m$, so $r < 2^{k-1}$. Similarly, when we apply Euclid's algorithm to n and r, we get $n = q_1 r + r_1$, where $r_1 < 2^{k-1}$. Therefore, when we apply Euclid's algorithm to r and r_1, it finds the greatest common divisor in at most $2(k-1)$ steps. Therefore, when we add the first two steps $m = qn + r$ and $n = q_1 r + r_1$, we have at most $2k$ steps in total. $\square$

6 In Sheet 4, Question 3 (a), you were asked to prove that any positive integer congruent to 3 modulo 4 is divisible by a prime that is also congruent to 3 modulo 4. You did this by contradiction, using the fact that the product of any collection of primes all congruent to 1 modulo 4 is also congruent to 1 modulo 4 (proving this requires induction). Now prove the same result by strong induction. [Hint: If n is prime, the result is obviously true. If not, then $n = ab$, where a and b must both be odd, $a > 1$ and $b > 1$, and one of them must be congruent to 3 modulo 4.]

Proof. Strong induction on n. If $n = 3$, then n is prime, so the result holds.

Now let $n \equiv 3 \pmod 4$ and suppose the result holds for all numbers less than n that are congruent to 3 modulo 4. We want to show that it holds for n. If n is prime, there is nothing to prove. If n is not prime, then $n = ab$ for positive integers a and b both greater than 1. Since n is odd, a and b must both be odd. If a and b were both congruent to 1 modulo 4, then their product n would also be congruent to 1 modulo 4, and it isn't, so at least one of a and b is congruent to 3 modulo 4 (in fact exactly one of a and b is congruent to 1 modulo 4). Without loss of generality, suppose $a \equiv 3 \pmod 4$. Now since $a < n$, by our induction hypothesis, a is divisible by a prime p satisfying $p \equiv 3 \pmod 4$. By transitivity of divisibility, $p|n$, so the result also holds for n. Therefore, by strong induction, it holds for all positive integers congruent to 3 modulo 4. $\square$

Bonus Question

7 *An $n \times n$ magic square is an $n \times n$ array containing each of the numbers $1, \ldots, n^2$ exactly once, such that every row, column and diagonal has the same sum. The following is a 3×3 magic square:*

2	*9*	*4*
7	*5*	*3*
6	*1*	*8*

Show that for any positive integer, k, there is a $3^k \times 3^k$ magic square.

Hint:

Call an $n \times n$ array a weak magic square if the sums of its rows, columns and diagonals are all the same. Try to get the $3^n \times 3^n$ magic square as a sum of weak $3^n \times 3^n$ magic squares.

For example, if you replace each entry of a magic square by a 3×3 array all containing the same number as that entry, then the result will be a weak magic square.