**MATH1061/7861 Assignment 4 Due 2pm Friday 4 April, 2008**

Complete all of questions 1, 2, 3, 4 and 5 and hand in your solutions by the due date and time. These questions are worth 2.5% towards your overall grade. **Make sure that your name, student number and tutorial group are on each sheet of your answers**. Question 6 is an extension question and is worth bonus marks. Should you answer this question correctly, you will receive an additional 1% towards your overall grade. Solutions to all the problems will be distributed later.

**1.** Consider the statement: "If the sum of any two real numbers is less than 50 then at least one of the numbers is less than 25".

- **(a)** Write the statement in symbolic form.
- **(b)** Write the negation of the statement in symbolic form.
- **(c)** Write the contrapositive of the original statement in symbolic form.
- **(d)** Prove that the original statement is true.

**2.** Show that each of the following statements is false.

- **(a)** The sum of any two irrational numbers is irrational.
- **(b)** The product of any rational number and any irrational number is irrational.
- **(c)** $\forall x \in \mathbb{Z}$ (with $x \neq 0$), $x^2 > x$.

**3.** Let $x$ be any rational number, $k$ be any non-zero rational number, and $y$ be any (non-zero) irrational number. Prove that $x + ky$ is irrational.

**4.** **(a)** Use the Euclidean Algorithm to find $\gcd(72, 164)$.

**(b)** Then *either* find integers $x$ and $y$ so that $164x + 72y = 6$,
*or else* find integers $s$ and $t$ so that $164s + 72t = 40$.
If either of these choices is not possible, explain briefly why.

**5.** Most secure electronic communication done over the internet uses a fascinating cryptosystem called *RSA* to encrypt data. RSA was developed within the last 30 years, yet it relies heavily on mathematical algorithms that have been known for thousands of years.

Two numbers $a$ and $b$ are said to be *relatively prime* if $gcd(a, b) = 1$. RSA operates by secretly selecting two large prime numbers $p$ and $q$, then selecting another number $r$ such that $r$ is relatively prime to $(p-1)(q-1)$. Show that the primes $p = 4723$ and $q = 8161$ and the number $r = 65537$ are valid choices of keys for RSA.

**6.** BONUS QUESTION (worth an extra 1% towards your final grade)
Let $k$ be an integer such that $k \geq 3$. Consider the following linear Diophantine equation.

$$(k-1)x + (k-2)y = (k+1)(k-2).$$

- **(a)** Find $\gcd(k-1, k-2)$.
- **(b)** Hence or otherwise show that integer solutions for $x$ and $y$ exist.
- **(b)** Find all integer solutions for $x$ and $y$ such that $x \geq 0$ and $y \geq 0$.

*(the end)*