NUI GALWAY MATHEMATICS ENRICHMENT PROGRAMME
MARCH 6 2010

Dr Rachel Quinlan
Rachel.Quinlan@nuigalway.ie

Number Theory could be described (for our purposes) as the study of the integers and their properties. The integers are the "whole" numbers. The set of integers is denoted $\mathbb{Z}$, that is

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}.$$

Note that the sum and product of two integers is always an integer. It is not always possible to divide one integer by another and get an integer as the result. However, if we divide an integer n by a (positive) integer m, we get an integer quotient q and a *remainder* r which is an integer between 0 and $m-1$. For instance if we "divide" 35 by 8 in $\mathbb{Z}$, we get a quotient of 4 and a remainder of 3.

Note : A (non-negative) integer is called a *square* if it is the square of an integer. The sequence of squares begins

$$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400, \dots$$

Some problems involving squares

1. Could the number 364514328991005432 be a square? No calculators!
2. Show that a square cannot have any of the following forms for an integer n
$$3n + 2,\ 5n + 3,\ 7n + 5.$$
3. If n is the sum of two squares, show that $2n$ is also.
4. Prove that the product of four consecutive integers is always one less than a perfect square. (BMO 1965)
5. The four-digit number with digits $aabb$ is a square. Find it.
6. From Edwin's session on February 20 : can any number in the sequence
$$11,\ 111,\ 1111,\ 11111,\ \dots$$
be a square?

Divisibility and Congruence

If the remainder on dividing an integer n by an integer m is zero, we say that m divides n and write $m|n$. So for example $5|20$, $11|88$, $3|72$, etc.

If two integers a and b have the same remainder upon division by a positive integer m, we say that a and b are *congruent to each other modulo m* and write

$$a \equiv b \mod m.$$

Note that this happens if and only if m divides the difference $a - b$. For example

$$21 \equiv 11 \mod 5,\ 42 \equiv 18 \mod 8,\ 392 \equiv 2 \mod 10,\ \text{etc.}$$

Every positive integer is congruent modulo 5 to exactly one of $0, 1, 2, 3, 4$. For example

$$23 \equiv 3 \mod 5,\ 49 \equiv 4 \mod 5,\ 500 \equiv 0 \mod 5.$$

In fact every positive integer is congruent modulo 5 to its remainder upon division by 5 (the same is true if we replace 5 with any positive integer m).

Some problems involving congruences

7. Show that among any four integers is a pair whose difference is a multiple of 3.
8. Show that 6 divides $n^3 + 5n$ for every integer n.
9. Let a and b be integers.
   (a) Show that $3|(a^2 + b^2)$ if and only if $3|a$ and $3|b$.
   (b) Show that $7|(a^2 + b^2)$ if and only if $7|a$ and $7|b$.
10. For integers a, b and c, show that 6 divides $a^3 + b^3 + c^3$ if and only if 6 divides $a + b + c$.
11. Show that 6 divides $2^{57} - 2$.
12. What is the smallest integer t for which there exist integers $x_1, x_2, \ldots, x_t$ with $x_1^3 + x_2^3 + \cdots + x_t^3 = 2002^{2002}$? (shortlisted for IMO 2002).
13. Let n be a integer that is not a multiple of 2 or 5. Prove that there is a multiple of n in which every digit is 1.

Prime and Composite Integers

A positive integer p is called *prime* if $p \geqslant 2$ and the only positive integers that divide p are 1 and p itself. A *composite* integer is one which is greater than 2 and not prime. The sequence of primes is infinite and begins as follows :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$$

The *Fundamental Theorem of Arithmetic* states that every integer from 2 onward can be expressed in a unique manner as a product of primes.

Some More Problems

14. Prove that if n is a non-negative integer, then $19 \times 8^n + 17$ is not a prime number.
15. If $p_1, p_2, \ldots, p_n$ are the first n primes, and p is their product, show that neither $p - 1$ nor $p + 1$ can be a square.
16. Suppose that a and b are positive integers with $a|b$. Prove that $2^a - 1|2^b - 1$.
17. Prove that the sequence defined by $a_n = \sqrt{24n + 1}$ contains all primes except 2 and 3.
18. Find all integers x, y for which $x + y = xy$.
19. Find all integers x, y for which $x^2 + xy + y^2 = x^2y^2$.
20. Find all integers x, y, z for which $x^2 + y^2 + z^2 = x^2y^2$.
21. Find all integers x, y, z for which $x + y = x^2 - xy + y^2$.
22. (a) Give an example of a positive integer n for which $2n + 1$ and $3n + 1$ are both squares.
    (b) Show that if $2n + 1$ and $3n + 1$ are both squares for some positive integer n, then $5n + 3$ is not a prime.