MATHS ENRICHMENT IN GALWAY
NUMBER THEORY I WORKSHEET
FEBRUARY 20, 2010

Listen to, collaborate and be constructive with, your fellow group members! And have fun!

Most of the problems here are well known throughout the maths enrichment world. However, the treatment here closely follows Zawaira's and Hitchcock's "A primer for mathematics competitions."

Tests for divisibility

Using the cases of 2,5, and 9 as inspiration, complete the following statements:

(1) A positive integer N is divisible by 4 $\Leftrightarrow$
(2) A positive integer N is divisible by 8 $\Leftrightarrow$
(3) A positive integer N is divisible by 6 $\Leftrightarrow$
(4) A positive integer N is divisible by 10 $\Leftrightarrow$
(5) A positive integer N is divisible by 11 $\Leftrightarrow$
(6) A positive integer N is divisible by 12 $\Leftrightarrow$

Bonus question Show that a positive integer N is divisible by 7 $\Leftrightarrow$ the smaller number M is divisible by 7, where M is the number formed by $2a_0$ subtracted from $a_n a_{n-1} \dots a_2 a_1$. For example if $N = 343$ then $M = 34 - 2(3) = 28$.

Question Find the unique factorization of $N = 47292$. (You may have to use the result of the above bonus question)

Finding remainders

We begin with the rules of modular arithmetic: We say that $a \equiv b (\bmod m)$ if m divides the quantity $a - b$. For every integer x we have the following:

(1) $(a + x) \equiv (b + x)(\bmod m)$ **(prove this)**
(2) $(a - x) \equiv (b - x)(\bmod m)$
(3) $(ax) \equiv (bx)(\bmod m)$
(4) $(a^n) \equiv (b^n)(\bmod m)$ for all positive integers n **(let's prove this together)**

Letting $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$ we also have

(1) $a + c \equiv (b + d)(\bmod m)$
(2) $a - c \equiv (b - d)(\bmod m)$
(3) $(ac) \equiv (bd)(\bmod m)$ **(let's prove this together)**

The key step used in showing that $5^{4000} \equiv 2 (\mathrm{mod}\, 7)$ was that $5^6 \equiv 1 (\mathrm{mod}\, 7)$ and so for all powers of 5^6 we had $(5^6)^t \equiv 1^t (\mathrm{mod}\, 7) \equiv 1 (\mathrm{mod}\, 7)$. Keep this in mind when answering the following:

(1) Find the remainder of 2^{4901} when it is divided by 11?.
(2) What are the last two digits in 11^{111}?

Fermat's Little Theorem

If p is a prime number and if a is *relatively prime* to p (that is, a and p do not have any common factors except 1) then:

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p) \text{ and also } a^p \equiv a (\mathrm{mod}\, p)$$

In other words, $a^{p-1} - 1$ is a multiple of p and so is $a^p - a$ since $a^p - a = a(a^{p-1} - 1)$. For example, if we choose $a = 8$ and $p = 3$ then $a^{p-1} - 1 = 8^{3-1} - 1 = 63 = 3 \times 21$.

(1) Find the remainder of 3^{1999} when it is divided by 47?.
(2) Try again to *Find the remainder of* 2^{4901} *when it is divided by* 11 but using Fermat's Little Theorem this time.

Unique factorization

We mentioned at the start of class today that: any positive integer N can be written in precisely one way in the form

$$N = p_1^{z_1} p_2^{z_2} p_3^{z_3} \cdots p_k^{z_k}$$

where $p_1, p_2, \ldots, p_k$ are prime, $p_1 < p_2 < \cdots < p_k$ and $z_1, z_2, \ldots, z_k$ are positive integers.

(1) Let N be a positive integer such that $\frac{N}{5}$ is a perfect square and $\frac{N}{2}$ is a perfect cube. Find the smallest number N for which $\frac{N}{3^3}$ is a positive integer.
(2) Using nique factorization, show that there do not exist positive integers a and b such that $\sqrt{2} = \frac{a}{b}$.

Parting problem: The Chinese remainder theorem

A duck knew was able to count the least number of ducklings she had by counting as follows: when counted in fives, 2 ducklings remained; when counted in threes, 2 ducklings remained; when counted in elevens, 3 ducklings remained. How many ducklings do you think she had?

Parting problem: Perfect squares

Is there ever a perfect square in the sequence $11, 111, 1111, 11111, 111111, 1111111, \ldots$