MODULAR ARITHMETIC II

MATH CIRCLE (INTERMEDIATE) 4/29/2012

A *Diophantine equation* is an equation with integer coordinates, for which we only want integer solutions.

1) Solve the following Diophantine equations.

a) $3x + 4y = 5$.

b) $3x + 6y = 5$.

c) $4x + 6y = 14$.

2) Solve the following Diophantine equations.

a) $(2x + y)(5x + 3y) = 7$.

b) $xy = x + y + 3$.

c) $x^2 + y^2 = x + y + 2$.

3) Solve the following Diophantine equations.

a) $x^2 - 7y = 10$.

b) $12x^2 - 5y^2 = 9$.

c) $3^m + 6 = 2^n$.

4) Let $ka \equiv kb(\mod m)$ where k and m are relatively prime. Prove that $a \equiv b(\text{mod} m)$

Fermat's Little Theorem:

Let p be a prime, and A not divisible by p. Then $A^{p-1} \equiv 1(\text{mod} m)$.

5) a) Find the remainder when 3^{102} is divided by 101.

b) Prove that $300^{3000} - 1$ is divisible by 1001.

5) a) Suppose n is not divisible by 17. Show that either $n^8 + 1$ or $n^8 - 1$ is divisible by 17.

b) Let p be prime, and suppose p does not divide a. Show that there is some b such that $ab \equiv 1 \text{mod} p$.

6) Prove that "Freshman's Dream": if p is prime, then $(a + b)^p \equiv a^p + b^p \text{mod} p$.

Challenge 0) Suppose the sum of $a + b + c$ is divisible by 30. Prove that $a^5 + b^5 + c^5$ is divisible by 30.

Challenge 1) Solve the Diophantine equation $3 \cdot 2^m + 1 = n^2$.

Challenge 2) Come up with a general method to solve the Diophantine equation $Ax + By = C$. Prove your result!

Challenge 3) Prove Fermat's Little Theorem.

Problems are taken from:

- D. Fomin, S. Genkin, I. Itenberg "Mathematical Circles (Russian Experience)"
- Previous UCLA Math Circle notes