Playsheet 5
Codes

MATH 130-02
Thursday, February 5, 2009

Directions: Groups should consist of three or four people. Work together on each problem; do not delegate different problems to different people. Submit one **neatly written** write-up per group. Remember to use complete sentences as appropriate and explain your reasoning. That is, **show your work!**

1. Decode the following message.

   PM P OHK H UPJRLS MVY LCLYF APTL ZVTLVUL ZHPK, "P OHAL THAO,"

   P JVBSK YLAPYL. P DVBSK IF MHY YHAOLY OHCL AOL UPJRLS, VY, ILAALY

   FLA, OHCL AOLT SVCL THAO HZ P KV.

2. (a) Compute $1^6, 2^6, 3^6, 4^6, 5^6, 6^6 \mod 7$.

   (b) Compute $1^{12}, 2^{12}, 3^{12}, \ldots, 11^{12}, 12^{12} \pmod{13}$.

   (c) Compute $1^5, 2^5, 3^5, 4^5, 5^5 \mod 6$.

   (d) Make a conjecture based on your computations from (a), (b), and (c).

(OVER)

3. Let $p = 11, q = 17$.

   (a) Compute $m = pq$.

   (b) Compute $(p-1)(q-1)$.

   (c) Let $e = 23$. Encode "5" by computing $5^e \mod m$. Call this number a.

   (d) Find a number d such that $de \mod (p-1)(q-1) = 1$. (This will take some trial and error.)

   (e) Compute $a^d \mod m$. What do you notice?