Math 455.1 **Homework Set 6** **Spring, 2009**

Corrected: 5 April 2009

Due: Monday, April 13 (start of class)

- Work either in a team or individually.
- For *Mathematica* work here, turn in printed pages. Try to place associated written work directly onto such printed pages (or include text cells there).
- For RSA systems, follow all our conventions: letters should be encoded into integers in $\{0, 1, 2 \ldots, 25\}$ as usual; and consecutive pairs of the resulting integers should be joined into 2-digit to 4-digit integers before encryption is applied.

1. Use the method shown in class, applying Fermat's Little Theorem, to find each of the following modular powers of 8 as efficiently as possible—*without* first actually computing 8 to the given powers.

   (a) $8^{2003} \bmod 7$

   (b) $8^{2003} \bmod 17$

2. Already known (and proved in class):

   Proposition 1. *If c is relatively prime to m, then $[c]$ has a multiplicative inverse in $\mathbb{Z}_m$.*

   Corollary 1. *If m is prime, then every nonzero element of $\mathbb{Z}_m$ has a multiplicative inverse.*

   Prove the following two converses of those results:

   Proposition 2. *If $[c]$ has a multiplicative inverse in $\mathbb{Z}_m$, then c is relatively prime to m.*

   (*Suggestion to get started:* Assume that $[c]$ has a multiplicative inverse in $\mathbb{Z}_m$. Express this in terms of a congruence modulo m.)

   Corollary 2. *If every nonzero element of $\mathbb{Z}_m$ has a multiplicative inverse, then m is prime.*

3. A bungling cipher bureau issues to Bob the public RSA key $(n, e) = (3239, 17)$ (which is rather insecure). Assist Alice by encrypting the following message that she wants to send Bob to Bob.

   ```
   What's another word for Thesaurus?
   ```

4. (a) Starting with the primes $p = 41$ and $q = 67$, generate for Bob a suitable RSA public key (n, e) with e as small as possible and yet satisfying the usual requirements.

   (b) Help Alice send the number 2418 securely to Bob: use that public key of Bob's to encrypt the number.

(c) Calculate Bob's private key.

(d) Decrypt for Bob the encrypted number from (b) that Alice sent him.

5. (*Corrected from the version originally posted.*)

   Alice uses the RSA system to encrypt a message and sends to Bob the following list of ciphertext numbers:

```
 274, 1412,  420, 1646,  539,  226,    1, 2143,
2180,  810, 1466, 1367, 1834, 1995, 2277, 1130,
1766, 1817, 1421,  293,  810, 1466, 1461,  591
```

   Bob's private key is $(n, d) = (2573, 17)$. Decipher Alice's message for Bob (into English words).

   For your convenience, that list of ciphertext numbers appears in notebook `Set6#5.nb`.

6. A cipher bureau issues to Alice the public RSA key $(n, e) = (2226295933, 52109)$. Show why that's a bad key by deducing Alice's corresponding private key.

   For your convenience, that public key appears in notebook `Set6#6.nb`.

7. [*Extra credit!*] *Without* using Euler's Theorem, deduce from Fermat's Little Theorem and/or other results:

   Corollary 3 (Euler's Corollary). *Let p and q be distinct primes and let a be an integer divisible by neither p nor q. Then:*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

   [*Note:* Since $\phi(pq) = (p-1)(q-1)$, the desired result is a special case of Euler's Theorem: $a^{\phi(m)} \equiv 1 \pmod{m}$ when $\gcd(a, m) = 1$.]