**Mathematics 360** **Homework (due Sep 11)** A. Hulpke

**6)** Using the fast powering algorithm, calculate $2^{477} \bmod 1000$. (Note: $477_{10} = 111011101_2$)

**7)** Suppose that $g, a, b, m$ are integers such that $g^a \equiv 1 \pmod{m}$ and $g^b \equiv 1 \pmod{m}$. Show that $g^{\gcd(a,b)} \equiv 1 \pmod{m}$.

**8)** We have that $4^{16} \equiv 1 \pmod{17}$. Can you conclude that $\mathrm{ord}_{17}(4) = 16$? (Your task is to write one or two sentences of explanatory text.)

**9)** a) Calculate $2^{1643} \bmod 1643$. Conclude from Fermat's little theorem that 1643 is not a prime. (Note: $1643_{10} = 11001101011_2$.)
b) Show that $a^{561} \equiv 1 \pmod{561}$ for $a = 2, 3, 4, 5$. (We have that $561_{10} = 1000110001_2$.)
One can show that this is true for all $a \in \{2, 3, \ldots 560\}$. Does this imply that 561 is a prime? Why or why not?

**10)** Bob and Alice have chosen a secret prime $k$, and encrypt messages $a$ by calculating $m = k \cdot a$ and sending this product. (I.e. decryption would be by calculating $m/k$.)
Eve managed to intercept two encrypted messages: $m_1 = 47444254$ and $m_2 = 59466841$. Calculate $\gcd(m_1, m_2)$, using the Euclidean algorithm. Can you decrypt (i.e. get the numbers that were the messages)?

**11)** Calculate $R = C \bmod 169$ where $C$ is your CSUID number. We will be using this remainder $R$ to assign individualized homework problems without disclosing your CSUID number.

On the course homepage you will find (link under homework 2 or `http://www.math.colostate.edu/~hulpke/lectures/m360/prob11.html`) a list of text snippets that have been encrypted with a Caesar cipher (i.e. shifting letters all in a row), together with frequencies of the occurring letters. (The texts are taken from *Winnie the Pooh* by A.A.Milne. They have been selected to be reasonably close to letter frequencies as listed in table 1.3 in the textbook.)
Find the snipped that belongs to your (CSUID mod 169) and decrypt it.

**Example:** For a student for whom CSUID mod 169 equals zero, the problem is:

```
CDUID mod 169: 0

WVVOH SDHFZ SPRLK HSPAA SLZVT LAOPU NHALS LCLUV JSVJR PUAOL
TVYUP UNHUK OLDHZ CLYFN SHKAV ZLLYH IIPAN LAAPU NVBAA OLWSH
```

| Letter: | L | A | H | V | S | U | P | O | N | Z | Y | K | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Freq: | 4.3 | 3.6 | 3 | 2.6 | 2.6 | 2.3 | 2.3 | 1.6 | 1.6 | 1.3 | 1 | 1 | 0.6 |
| Letter: | D | C | W | T | R | J | I | B | M | Q | X | E | G |
| Freq: | 0.6 | 0.6 | 0.6 | 0.6 | 0.6 | 0.6 | 0.6 | 0.3 | 0 | 0 | 0 | 0 | 0 |

As L is most frequent we may guess that this will correspond to E. Thus L is E, M is F, H is A and so on. We decipher the text as

```
POOHA LWAYS LIKED ALITT LESOM ETHIN GATEL EVENO CLOCK INTHE
MORNI NGAND HEWAS VERYG LADTO SEERA BBITG ETTIN GOUTT HEPLA
```

or (adding spaces and punctuation)

> *Pooh always liked a little something at eleven o'clock in the morning, and he was very glad to see Rabbit getting out the pla[tes]*

**Practice Problems:** (These problems from the book are not to be handed in, but might be useful in reviewing and in exam preparation): **1.28**, **1.30**, **1.32**,