**CS 310-0**
**Homework Assignment No. 7**
Due Fri 3/3/2000

1. If $p$ is a prime number, prove that $\binom{p}{k} \equiv 0 \pmod{p}$ for every $0 < k < p$. Then prove the following (rather trivial) form of the binomial theorem:
$$(x+y)^p \equiv x^p + y^p \pmod{p}\,.$$

2. Prove that the following Diophantine equation has no positive integer solutions:
$$x^3 + 4\,y^3 = 7\,z^3\,.$$
(Hint: think modulo some appropriate $m$.)

3. Consider the function $f(x) = x^2 - 3\,x + 2$. Find all integers $x$ such that $f(x)$ is a multiple of 12, i.e., solve the congruence:
$$x^2 - 3\,x + 2 \equiv 0 \pmod{12}\,.$$
(Hint: You may start by solving the equation $f(x) = 0$ on $\mathbb{Z}_{12}$.)

4. Let $m$ be an integer greater than 1 and relatively prime to 10. Then $1/m$ has a non-terminating periodic decimal representation. Let $l_{10}(m)$ be the length of the period in the decimal representation of $1/m$—e.g., $1/7 = 0.142857142857\ldots \Rightarrow l_{10}(7) = 6$, $1/11 = 0.09090909\ldots \Rightarrow l_{10}(11) = 2$, etc. Prove:
(a) $l_{10}(m) = \min\{n \in \mathbb{Z}^+ \mid 10^n \equiv 1 \pmod{m}\}$.[1]
(b) If $n \in \mathbb{Z}^+$ then $10^n \equiv 1 \pmod{m} \Leftrightarrow l_{10}(m) \mid n$. In particular $l_{10}(m)$ divides $\phi(m)$, where $\phi$ is Euler's phi function.
(c) If $p$ is a prime number different from 2 and 5, then either $l_{10}(p^2) = l_{10}(p)$ or $l_{10}(p^2) = p\,l_{10}(p)$.[2]

5. Let $N$ be the number $N = 4 \uparrow\uparrow 4 = 4^{4^{4^4}}$. Find the two rightmost digits of $N$ (in base 10).

6. A group of one thousand soldiers go to battle. After the fight their commander makes them form rows of 9 and notices that the last row has only 6 soldiers. Then he makes them form rows of 10 and they fit exactly. Then he makes them form rows of 11 and the last row ends up having only 1 soldier. How many soldiers were lost in the battle?

[1]Note that $l_{10}(m)$ is the minimum $n \in \mathbb{Z}^+$ such that $\frac{10^n}{m} - \frac{1}{m}$ is an integer.
[2]As a matter of fact for most primes $l_{10}(p^2) = p\,l_{10}(p)$, but there are some exceptions, for instance $l_{10}(9) = l_{10}(3) = 1$—can you think of other "exceptional" primes besides 3?

7. We have intercepted a secret message from the enemy encrypted with the RSA algorithm. The encoding is $A = 01, B = 02, C = 03, \ldots, Z = 26$, and the public encryption key used by the enemy is $(n, e) = (31764071, 17293841)$. For instance, the word $DOG$ would be encrypted as follows. First it is encoded: $DOG = 041507$. Then it is encrypted: $041507^{17293841} \equiv 19656874 \pmod{31764071}$. The encrypted message that we have intercepted is $m' = m^e = 30151919 \pmod{31764071}$. Your mission is to decrypt the message. In order to do that, use the following steps (you will need some computer algebra system such as Maple to do the computations):[3]
   1) Find the prime factors $p$ and $q$ of $n = 31764071$.
   2) Find $\phi(n)$.
   3) Find $d = e^{-1}$ in $\mathbb{Z}_{\phi(n)}$. The decryption key is $(n, d)$.
   4) Decrypt the secret message by computing $m'^d \equiv m \pmod{n}$.

[3] In Maple you may use "ifactor" to find the prime factors of $n$, and "mod" for computations modulo $n$. Remember to use the ampersand in expressions of the form "$a\&\hat{}\,b \mod n$" in Maple (so that Maple uses the efficient algorithm to compute powers modulo $n$.) Basically, the computations to be performed are: find $p$ and $q$ with "ifactor($n$)", find $\phi(n) =$ "$(p-1)*(q-1)$", find $d =$ "$e\&\hat{}(-1) \mod \phi(n)$", find $m =$ "$m'\&\hat{}\,d$ mod $\phi(n)$". Finally, decode $m$.