SOAR Math Course Homework Four Spring, 2003

Homework Four

These homework problems are meant to expand your understanding of what goes on during class. Any you turn in will be graded and returned to you. Answers may or may not be posted on the web, depending on demand.

1. What is the last digit of 7^{213}? This sort of question is common in contests. This problem walks you through answering this question.
   (a) What we're asked for is $7^{213} \bmod 10$. Make a table with the values, modulo 10, of $7^1 = 7$, 7^2, 7^4, 7^8, 7^{16}, 7^{32}, 7^{64}, and 7^{128}. (We don't need 7^{256} as $213 < 256$.)
   (b) Write 213 as a sum of numbers from the set $\{1, 2, 4, 8, 16, 32, 64, 128\}$.
   (c) Write 7^{213} as a product of numbers from the set $\{7^1, 7^2, 7^4, 7^8, 7^{16}, 7^{32}, 7^{64}, 7^{128}\}$.
   (d) Use your table from part (a) to compute 7^{213} modulo 10.

2. Follow the process of the previous problem to find the last digit of the following numbers.
   (a) 3^{521}
   (b) $M_{4253} = 2^{4253} - 1$ (This is the 19th Mersenne prime, which are prime numbers of the form $M_p = 2^p - 1$.)
   (c) $F_5 = 2^{2^5} + 1$. (This is the first Fermat number that is not prime. Fermat numbers are those of the form $F_n = 2^{2^n} + 1$.)

3. We could apply the same procedures from the previous two problems to other bases other than 10. Commonly used bases are 2 (binary), 8 (octal), 12 ("clock"), and 16 (hexadecimal, where A is used for 10, B for 11, and so on up to F for 15). Thus, for example, 29 base 10 is 1D base 16. On the other hand, $29 \equiv 13 \bmod 16$, so the "last digit" when 29 is written in base 16 must be 13 = D.
   (a) Find the last digit of 3^{521} (base 10) when it is written base 8.
   (b) Find the last digit of 3^{521} (base 10) when it is written base 16.
   (c) Find the last digit of M_{4253} and F_5 when they are written base 16. (This is easier than it looks at first, and much easier than it was base 10.)

4. In this problem, we derive a formula for the Euler ϕ-function (also known as the *totient* function). Recall that this is defined as

$$\phi(n) = \text{the number of integers } k \text{ with } 0 < k < n \text{ and } \gcd(k, n) = 1.$$

   (a) Prove that for a prime p, $\phi(p^n) = (p-1)p^{n-1}$. (Hint: what are the integers $0 < k < p^n$ that have a common factor with p^n?)
   (b) (Hard, and I recommend you skip this part and just assume this for part (c).) Prove that ϕ is multiplicative. That is, if $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.
   (c) Derive a formula for $\phi(n)$. Your answer should involve the prime factorization of $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.
   (d) What is $\phi(238)$?
   (e) What is $\phi(2^7 \cdot 3^5 \cdot 11^2 \cdot 17)$?