CS5319 Advanced Discrete Structure

Homework 5

Due: 1:10 pm, December 09, 2010 (before class)

1. For each m greater than 1, how many primes are there in the closed interval $[m!+2, m!+m]$? Explain your answer.

2. Let p be a prime.

   (a) Suppose $xy \equiv 0 \pmod{p}$. Show that either $x \equiv 0$ or $y \equiv 0$ modulo p.

   (b) Show that if $1 < x < p-1$ and $xy \equiv 1 \pmod{p}$, then $y \not\equiv x \pmod{p}$.

   (c) Show that $2 \times 3 \times \cdots \times (p-2) \equiv 1 \pmod{p}$.

   (d) Conclude that Wilson's theorem is true. That is, $(p-1)! \equiv -1 \pmod{p}$.

3. Prove that if p is a prime congruent to 1 modulo 4, then

$$\left(\frac{p-1}{2}\right)!^2 \equiv -1 \pmod{p}.$$

   Hint: Show that $((p-1)/2)!^2 \equiv (p-1)! \pmod{p}$.

4. Prove that if $n^j \equiv 1 \pmod{m}$ and $n^k \equiv 1 \pmod{m}$, then

$$n^{\gcd(j,k)} \equiv 1 \pmod{m}.$$

   Hint: Properties of GCD.

5. A number n is a perfect number if the sum of all the proper divisors of n (i.e., all divisors excluding n itself) is exactly n. For instance, 6 and 28 are both perfect numbers, because

$$\begin{array}{lcll} \text{sum of proper divisors of 6} & = & 1+2+3 & = 6, \quad \text{and} \\ \text{sum of proper divisors of 28} & = & 1+2+4+7+14 & = 28. \end{array}$$

   In the following, we shall show an interesting result by Euler:

   Theorem 1. *An even number n is a perfect number if and only if $n = 2^m(2^{m+1}-1)$ and $2^{m+1}-1$ is prime.*

   (a) Prove that if $n = 2^m(2^{m+1}-1)$ and $2^{m+1}-1$ is a prime, then n is a perfect number.

   (b) Suppose n is an even number, so that we can express n as $2^m Q$ for some odd integer Q. Also, suppose $\sigma(Q)$ denotes the sum of all divisors of Q (i.e., including itself). Show that if n is a perfect number, then

$$2^{m+1}Q = 2n = (2^{m+1}-1)\sigma(Q).$$

   (c) Using the result from part (b), show that Q is a multiple of $2^{m+1}-1$.

   (d) Suppose that $Q = (2^{m+1}-1)q$. Show that the following is true:

$$2^{m+1}q = \sigma(Q) \geq q + Q = 2^{m+1}q.$$

   (e) Using the result from part (d), show that Q must be a prime and $Q = 2^{m+1}-1$. In other words, $n = 2^m Q = 2^m(2^{m+1}-1)$ for some prime $Q = 2^{m+1}-1$.

6. (Challenging: No marks) Show that for all $n > 1$, $2^n \not\equiv 1 \pmod{n}$.