Math 480 (Spring 2007): Homework 3

Due: Monday, April 16

There are 8 problems. Each problem is worth 6 points and parts of multipart problems are worth equal amounts.

1. Let φ be the Euler phi function. The first few values of φ are as follows (you do not have to prove this):

   ```
   1 1 2 2 4 2 6 4 6 4 10 4 12 6 8 8 16 6 18 8 12 10 22 8 20 12 18 12 28
   ```

   Notice that most of these numbers are even. *Prove for all $n > 2$ that $\varphi(n)$ is an even integer.* (You may using anything that is proved about φ in the course textbook.)

2. Compute each of the following *entirely by hand – no calculator.* In each case, given the problem $\mathrm{xgcd}(a, b)$, your final answer will be integers x, y, g such that $ax + by = g$. It is probably best to use the algorithm I described in class, which is also in the newest version of the course notes.

   (a) $\mathrm{xgcd}(15, 35)$

   (b) $\mathrm{xgcd}(59, -101)$

   (c) $\mathrm{xgcd}(-931, 343)$

   (d) $\mathrm{xgcd}(-123, -45)$

   (e) $\mathrm{xgcd}(144, 233)$

   (f) Find integers x and y such that $17x - 19y = 5$.

3. Do each of the following using any means (including a computer). As in the previous problem, your answer is integers x, y, g such that $ax + by = g$.

   (a) $\mathrm{xgcd}(2007, 2003)$

   (b) $\mathrm{xgcd}(12345, 678910)$

   (c) $\mathrm{xgcd}(2^{101} - 1, 2^{101} + 1)$

4. Prove that there are infinitely many composite numbers n such that for all a with $\gcd(a, n) = 1$, we have $a^{n-1} \equiv a \pmod{n}$. (Hint: consider $n = 2p$ with p an odd prime.)

5. Solve each of the following equations for x (you may use a computer if necessary):

   (a) $59x \equiv 5 \pmod{101}$

   (b) $144x + 1 \equiv 2 \pmod{233}$

   (c) $17x \equiv 18 \pmod{19}$

6. Prime numbers p and q are called *twin primes* if $q = p + 2$. For example, the first few twin prime pairs are

$$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103),$$

and it is an open problem to prove that there are infinitely many. Notice in the above list of pairs (p, q) that, *except for the first pair*, we have that $p+q$ is divisible by 12. Prove that if p and q are twin primes with $p \geq 5$, then $p + q \equiv 0 \pmod{12}$, as follows:

   (a) Prove that if $p \geq 5$ is prime, then $p \equiv 1, 5, 7, 11 \pmod{12}$, i.e., there are only four possibilities for p modulo 12.

   (b) Show that if p and $p + 2$ are both prime with $p \geq 5$, then $p \equiv 5 \pmod{12}$ or $p \equiv 11 \pmod{12}$.

   (c) Conclude that $p + q \equiv 0 \pmod{12}$.

7. Let $n = 323$. Do the following by hand:

   (a) Write n in binary, i.e., base 2.

   (b) Compute $2^{n-1} \pmod{n}$ by hand.

   (c) Is n prime. Why or why not?

8. Let $n = 167659$.

   (a) Use a computer to write n in binary. E.g., in SAGE, use `167659.str(2)`.

   (b) Use a computer to compute $2^{n-1} \pmod{n}$, e.g., in SAGE do `n=167659; Mod(2,n)^(n-1)`.

   (c) Is n prime?