Math 362 Assignment 3

Due: Wednesday, October 16

- Answer all questions. Each question is worth 5 marks. Full marks will be awarded only for answers that are both mathematically correct and coherently written.
- Please consider the markers and write neatly and legibly! I have instructed the markers to ignore work they cannot read. (And I won't read it, either.)

1. Use Wilson's Theorem to prove that if p is prime and $p \equiv 1 \pmod 4$, then

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

Note: Remember this problem!

Answer

Let p be prime and $p \equiv 1 \pmod 4$. By Wilson's Theorem, $(p-1)! \equiv -1 \pmod p$. Since $p \equiv 1 \pmod 4$, $p-1 = 4k$ for some positive integer k. Now we have

$$\begin{aligned}(p-1)! &\equiv (4k)(4k-1)\cdots(2k+1)(2k)(2k-1)\cdots 2\cdot 1 \pmod p\\ &\equiv (-1)(-2)\cdots(-(2k))(2k)(2k-1)\cdots 2\cdot 1 \pmod p\\ &\equiv (-1)^{2k}1\cdot 2\cdots(2k)(2k)(2k-1)\cdots 2\cdot 1 \pmod p\\ &\equiv (2k)! \pmod p.\end{aligned}$$

Since $2k = \frac{p-1}{2}$ and $(p-1)! \equiv -1 \pmod p$, it follows that

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

2. (a) [2] Find infinitely many integers n such that $d(n) = 65$. (One line!)

   (b) [3] Find four solutions of $\phi(n) = 16$.

Answer

(a) Since there are infinitely many primes we can choose $n = p^{64}$, where p is prime. Then $d(n) = 65$. (OK, this is 1 line $+\varepsilon$.)

(b) (i) Let p be prime. Then $\phi(p^r) = p^{r-1}(p-1)$.
For $n = p = 17$ where therefore have $\phi(n) = 16$.
For $n = 2^5$, $\phi(n) = 2^4 = 16$.
(ii) Suppose $n = p^r q^s$, where p and q are distinct primes. Then $\phi(n) = p^{r-1}(p-1)q^{s-1}(q-1)$.
For $n = 2 \cdot 17$, $\phi(n) = 16$.
For $n = 2^3 \cdot 5$, $\phi(n) = 2^2(5-1) = 16$
Hence the solutions are $n \in \{17, 32, 34, 40\}$.

3. *I'm changing the mark for this question from 5 to 3, and the mark for Questions 5 and 7 to 6.*

An integer n is called **triangular** if and only if $n = m(m+1)/2$ for some integer m. Prove that every even perfect number is triangular.

Answer

[3] If n is an even perfect number, we can write $n = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is prime. Let $m = 2^p - 1$. Then $m + 1 = 2^p$ and $n = m(m+1)/2$.

4. (a) [3] Let p be prime and let M_p denote the number $2^p - 1$. The number M_p is called a *Mersenne number*, and if it is prime, it is called a *Mersenne prime*. There is a test, called the **Lucas-Lehmer Test**, that gives a necessary and sufficient condition for M_p to be prime. It is always used to verify that a Mersenne number, suspected of being prime, is indeed a Mersenne prime. Give the statement of this test. Why is it a "fast" test for verifying primality?
(Look it up in a book or on the internet.)

(b) [2] Let p and q be odd primes. There is a necessary condition for q to divide M_p found by Fermat (one part) and Euler (the other part). State this condition. Follow the advice in (a).

Answer

(a) **The Lucas-Lehmer Test:** Let $S(n)$ be the sequence defined recursively by $S(1) = 4$ and $S(n+1) = [S(n)]^2 - 2$, $n \geq 1$. (The first four numbers in this sequence are 4, 14, 194, 37 634.)
For p an odd prime, the Mersenne number $2^p - 1$ is prime if and only if $S(p-1) \equiv 0 \pmod{2^p - 1}$.

The test is efficient because it can be performed without requiring factorization.
(The Lucas-Lehmer test is used by GIMPS (Great Internet Mersenne Prime Search) in the final stages of primality testing of Mersenne numbers.)

(b) If p is an odd prime and q is a prime such that $q|(2^p - 1)$, then $q = 2kp + 1$, where $k \in \mathbb{Z}^+$, and $q \equiv \pm 1 \pmod{8}$.

5. [6] Let k be a fixed positive integer. Show that if there is exactly one positive integer n such that $\phi(n) = k$, then $36|n$.

   [Hint: Assume $36 \nmid n$, write n as $n = 2^r 3^s m$, where $(m, 2) = (m, 3) = 1$, and consider the various possibilities for r and s.]

   Answer

   Proof by contradiction: Suppose n is the only positive integer such that $\phi(n) = k$, for some fixed $k \in \mathbb{Z}^+$, but $n \not\equiv 0 \pmod{36}$. Then we can write $n = 2^r 3^s m$, where $(m, 2) = (m, 3) = 1$, and $r < 2$ or $s < 2$.

   Since ϕ is multiplicative, it follows that

$$\phi(n) = \phi(2^r)\phi(3^s)\phi(m).$$

   Suppose $r = 0$ or $r = 1$. Let $n_0 = 3^s m$ and $n_1 = 2 \cdot 3^s m$. Then

$$\begin{aligned}\phi(n_1) &= \phi(2)\phi(3^s)\phi(m) = \phi(3^s)\phi(m) \quad \text{since } \phi(2) = 1\\ &= \phi(n_0).\end{aligned}$$

   Hence the equation $\phi(n) = k$ has two solutions: n_0 and n_1.

   Suppose $r \geq 2$. Then $r - 2 \geq 0$, hence 2^{r-2} is an integer. Also (since $\min\{r, s\} \leq 1$), $s = 0$ or $s = 1$. Let $n_0 = 2^r m$ and $n_1 = 2^r 3m$. Then

$$\phi(n_0) = \phi(2^r)\phi(m) = 2^{r-1}\phi(m) = 2^{r-2} \cdot 2 \cdot \phi(m) = \phi(2^{r-1})\phi(3)\phi(m) = \phi(2^{r-1}3m)$$

   and

$$\phi(n_1) = \phi(2^r)\phi(3)\phi(m) = 2^{r-1} \cdot 2 \cdot \phi(m) = 2^r\phi(m) = \phi(2^{r+1}m).$$

   Hence if $s = 0$, the equation $\phi(n) = k$ has the solutions n_0 and $2^{r-1}3m$, and if $s = 1$, then the equation has the solutions n_1 and $2^{r+1}m$.

6. The following message has been encrypted using a Caesar cypher with constant shift. What does it say?

   "AX USFSVS AK LG KMJNANW, AL USF GFDQ KMJNANW AF EMLMSD JWKHWUL SFV AF DGNW XGJ GFW SFGLZWJ."

   Answer

   Using the "two disc" method I described in class, or any other method, one soon discovers that a shift of 18 (or -8) has been used to encode the message. Decoding it by shifting 8 letters forward, one gets the message:

“If Canada is to survive, it can only survive in mutual respect and in love for one another.”

(Pierre Trudeau, October 18, 1919 – September 28, 2000; Canadian Prime Minister April 20, 1968 – June 4, 1979 and March 3, 1980 – June 30, 1984.)

7. [6] The following message has been encrypted using a Caesar cypher with random shift, each letter mapped to the same letter for every occurrence. (I.e., if “X” is mapped to “Y” in one instance, “X” is mapped to “Y” each time it occurs.) What does it say?

   “KO R QSOCSOIS, CVS MSXE VRQ CP RAXSS GKCV CVS QYEZSIC.”

   Answer

   The key is

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	E	I	J	S	U	A	V	K	Z	B	T	L	O	P	D	W	X	Q	C	Y	M	G	F	N	H

   and the message is

   “In a sentence, the verb has to agree with the subject.”